Markus Koskimäki

UUDEN MAKSUPALVELUDIREKTIIVIN TUOMAN VAHVAN TUNNISTAUTUMISEN OMAKSUMINEN JA VAIKUTUS MAKSUKÄYTTÄYTYMISEEN VERKKO-MAKSUISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Koskimäki, Markus
Uuden maksupalveludirektiivin tuoman vahvan tunnistautumisen omaksuminen ja vaikutus maksukäyttäytymiseen verkkomaksuissa
Jyväskylä: Jyväskylän yliopisto, 2022, 59 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Frank, Lauri

Verkkokauppojen maksuvälineet ovat kehittyneet viime aikoina nopeasti ja Euroopan unioni (EU) on halunnut tuoda kuluttajille turvaa verkkomaksamisessa. EU sääti maksupalveludirektiivistä toisen version PSD2:n (Payment Services Directive 2), jossa vahva tunnistautuminen tuli osaksi verkkomaksamista. Uutena asiana se tuli käytännössä vain pankkikorttimaksuihin, sillä muut maksuvälineet sisältävät jo entuudestaan vahvan tunnistautumisen. Tässä tutkielmassa tutkin vahvan tunnistautumisen omaksumisen kokemuksia kuluttajilta, jotka käyttävät verkkokauppaa arjessaan. Tutkimukseen osallistui kahdeksan nuorta aikuista, joille verkkokauppa ja pankkikortilla verkossa maksaminen on tuttua.

Tutkimus on toteutettu kahdessa eri osassa, aluksi kirjallisuuskatsaus, jossa käsitellään teoriaviitekehystä UTAUT2-mallia ja sovelletaan sitä tähän tutkimukseen. Sitten tutkitaan kirjallisuutta maksuvälineistä ja maksupalveludirektiivistä. Toinen osa oli empiirinen tutkimus, joka toteutettiin puolistrukturoituna haastatteluna ja saatu aineisto analysoitiin fenomenografisella analyysilla.

Tutkimuksen tulokset osoittivat, että vahva tunnistautuminen on koettu helppokäyttöiseksi, mutta samalla se on koettu turhauttavaksi, koska pankkikorttimaksu koetaan olevan nykyään turha maksuväline sen pitkän maksuprosessin vuoksi. Vahva tunnistautuminen on otettu kaikesta huolimatta kuluttajien käyttöön normaalina asiana, joka kuuluu prosessiin. Tutkimuksen tulokset osoittivat myös, että on myös niitä, jotka yrittävät välttää mahdollisuuksien mukaan vahvaa tunnistautumista. Haastatteluiden perusteella vahva tunnistautuminen on koettu vähentäneen haastateltavien pankkikorttimaksamista verkkokaupoissa. Lisäksi haastateltavat ovat suosineet mobiilimaksamista sen jälkeen, kun vahva tunnistautuminen on tullut osaksi verkkomaksamista.

Asiasanat: verkkokauppa, vahva tunnistautuminen, maksuvälineet, teknologian omaksuminen, UTAUT2, PSD2

ABSTRACT

Koskimäki, Markus
Adoption of the strong authentication introduced by the new Payment Services Directive and its impact on payment behavior in online payments
Jyväskylä: University of Jyväskylä, 2022, 59 pp.
Information system science, Master's Thesis
Supervisor(s): Frank, Lauri

E-commerce payment methods have evolved recently, and the European Union (EU) is willing to improve the security to consumers when paying online. The EU enacted a second version of the Payment Services Directive, PSD2, in which strong authentication became part of online payment. As an addition it only came to credit and debit cards payments in practice, as other means of payment already contain strong authentication. In this thesis, I am going to explore experiences of strong authentication from consumers who use e-commerce in their daily lives. Eight young adults, who are familiar with e-commerce and online debit payments, participated in the study.

The thesis was carried out in two different parts. Firstly, the literature review was carried out of UTAUT2 model and the theoretical framework and applies it to this study. The literature on payment instruments and the Payment Services Directive is then examined. Secondly empirical research was done by conducting semi-structured interview and the data which was obtained analyzed by phenomenographic analysis.

The results of the study showed that strong authentication has been perceived as easy to use, but at the same time it has been perceived as frustrating, as debit card payments are now perceived as a useless payment instrument due to its long payment process. Strong authentication has nevertheless been introduced to consumers as a normal part of the process. The results of the study also showed that there are also those who try to avoid strong authentication where possible. Based on the interviews, strong authentication has been felt to have reduced the interviewees' debit card payments in online shopping. In addition, interviewees have favored mobile payment after strong identification has become part of online payment.

Keywords: e-commerce, strong customer authentication, online store payment methods, technology adoption, UTAUT2, PSD2

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Verkkokaupoista ostaminen on yleistynyt merkittävästi viime vuosien aikana (Sintonen, Takala, Hellqvist & Liikanen, 2021; SVT, 2021a). Myös Euroopan unioni on huomioinut tämän trendin ja on asettanut uuden maksupalveludirektiivin PSD2:n (Payment Service Directive 2). Direktiivin yhtenä säännöksenä verkkomaksuihin tuli pakollinen vahva tunnistautuminen ja tämän seurauksena kaikki pankkikortilla tehdyt verkko-ostokset täytyy erikseen vahvistaa tunnistautumalla verkkopankkitunnuksilla. Maksupalveludirektiivi astui voimaan jo syyskuussa 2019, mutta direktiivin sisältämälle pankkikorttimaksujen uudistukselle annettiin aikaa vuoden 2020 loppuun saakka. Direktiivin tarkoituksena on tuoda maksupalvelut sääntelyn piiriin ja kehittää sääntelyä kehittyvien markkinoiden mukaan. (Finanssivalvonta, 2019c) Tässä tutkielmassa perehdytään suomalaisten kuluttajien kokemukseen vahvan tunnistautumisen käyttöönotosta ja siihen, miten se on vaikuttanut kuluttajien maksukäyttäytymiseen verkkokauppojen maksutapahtumassa.

Kuluttajan kannalta uudistus on tuonut turvallisuutta maksamiseen. Enää ei pysty pelkällä pankkikorttiin painetuilla tiedoilla tekemään verkko-ostoja, kun siihen tarvitaan vahva tunnistautuminen kortin tietojen lisäksi. Tämän johdosta myös jokainen verkkomaksu on entistä työläämpi. Nykyään käyttäjät suosivat käteviä ja helppoja maksutapoja (Zhong, Oh & Moon, 2021), joten vahva tunnistautumisen myötä pankkikorttimaksut eivät ole kovin suosittuja, vaan melko turhia, koska vahva tunnistautuminen tehdään pankkitunnuksilla ja se on käytännössä sama prosessi, joka tehdään verkkopankkimaksussa. Osittain myös tästä syystä kuluttajat ovat viime vuosina ottaneet enenevissä määrin käyttöön uusia maksutapoja, kuten mobiilimaksamisen, joka koetaan helppona maksutapana. Mobiilimaksaminen on silti vielä lähtökuopissaan ja ei ole vielä haastamassa perinteisiä maksutapoja yleisimpänä maksutapana (Sintonen ym., 2021). Maksutapojen trendi tulee olemaan tulevaisuudessa pitkälti mobiililaitteiden kehityksen mukaista (Alhonen, 2015).

Direktiivi on muuttanut verkkokauppojen maksutapahtumaa niin paljon, että kyseistä aihetta on hyvä tutkia. Lisäksi aihe on uusi ja siksi vahvan tunnistautumisen omaksumista ja sen vaikutusta maksukäyttäytymiseen ei ole tutkittu tarpeeksi. Tutkimusta on paljon erilaisista vahvoista tunnistautumistavoista ja sovelluksista (Abbott & Patil, 2020; Bartłomiejczyk, El Fray, Kurkowski, Szymoniak & Siedlecka-Lamch, 2022), mutta pankkikorttimaksujen vahvaa tunnistamista ei ole tutkittu sen omaksumisen kannalta. Tämän tutkielman tavoitteena on selvittää, miten vahva tunnistautuminen on kuluttajien toimesta omaksuttu ja miten sen koetaan muuttaneen maksukäyttäytymistä. Tutkimuskysymykset ovat:

- Miten kuluttajat ovat kokeneet vahvan tunnistautumisen käyttöönoton?

- Miten vahvan tunnistautumisen on koettu vaikuttavan maksukäyttäytymiseen?

Tutkielman aiemman tutkimuksen hyödyntäminen toteutetaan kirjallisuuskatsauksena. Tietokantoina käytetään pääosin Google Scholaria ja JYKDOKia. Hakusanoina tutkielman lähteiden hakemiseen käytin muun muassa seuraavia: e-commerce, online store payment methods, technology adoption, psd2 payments, strong customer authentication, user experience ja user authentication. Lisäksi hain tietoa muun muassa finanssivalvonnan ja Euroopan komission verkkosivuilta sekä Paytrailin kyselytutkimuksista.

Tutkielman toisessa luvussa tutkitaan aiempaa kirjallisuutta teknologian hyväksymisestä. Teoriaviitekehyksenä ovat teknologian hyväksymismalli, TAM (Technology Acceptance Model), sekä teknologian hyväksymisen ja käytön yhdistettyä teoria, UTAUT2 (Unified Theory of Acceptance and Use of Technology). Ne ovat tutkielman runkona ja käyn niiden mallien kautta läpi vahvan tunnistautumisen käyttöönottoa ja omaksumista, sekä toteutan tutkimuksen niihin pohjautuen. TAM-malli on kehitetty tutkimaan teknologian vaikutusta käyttäjän käyttäytymiseen ja sillä pyritään ennustamaan käyttäjän uuden teknologian ja teknologisten ominaisuuksien omaksumista (Davis, 1989). UTAUT2-malli on TAM-malliin pohjautuva teoria, joka ottaa huomioon monia muitakin tekijöitä teknologian omaksumisessa (Venkatesh, Thong & Xu, 2012).

Kolmannessa luvussa tutkitaan maksuvälineistä tehtyä tutkimusta. Lisäksi tässä luvussa vertaillaan maksuvälineitä niiden käyttöosuuksien ja toiminnan perusteilla. Tutkielmassa keskeisenä osana on Euroopan unionin toinen maksupalveludirektiivi PSD2, jota käsitellään luvussa neljä. Uuden maksupalveludirektiivin mielenkiinto kohdistuu tässä tutkielmassa vahvaan tunnistautumiseen. Maksupalveludirektiivistä etsin tietoa niin Euroopan komission verkkosivuilta kuin Suomen finanssivalvonnan verkkosivuilta.

Tutkielman empiirinen osuus on toteutettu puolistrukturoiduilla haastatteluilla. Luvussa viisi kerrotaan tarkemmin haastattelun suunnittelusta ja toteutuksesta. Haastateltavat olivat nuoria, verkkokauppaa paljon käyttäviä kuluttajia, joilla on kokemusta verkkoostoista ennen ja jälkeen vahvan tunnistamisen tulemista pakolliseksi verkkokaupan maksutapahtumiin.

2 TEKNOLOGIAN OMAKSUMISMALLIT

Teknologian omaksumismallit ovat yleisesti käytettyjä malleja tietojärjestelmätieteen tutkimuksissa. Omaksumismalleissa tutkitaan, miksi ihmiset ottavat jonkun teknologian käyttöön tai miksi ei ota. Teknologian omaksumisen tutkimisesta on tullut yksi tietojärjestelmätieteen päälinja. (Rondan-Cataluña, Arenas-Gaitán & Ramírez-Correa, 2015). Niiden avulla voidaan ennustaa käyttäjien hyväksyntää erilaisille teknologioille (Davis, 1989). Tässä tutkimuksessa teoriaviitekehyksenä käytän Davisin vuonna 1989 luomaa teknologian hyväksymismallia TAM:ia (Technology Acceptance Model) sekä Venkateshin, Morrisin, Davisin ja Davisin vuonna 2003 luomaa teknologian hyväksymisen ja käytön yhdistettyä teoriaa, tarkemmin ottaen sen toista versiota, joka lyhennetään UTAUT2 (Unified Theory of Acceptance and Use of Technology). Lisäksi käyn läpi TAM-mallin perustan, joka on perustellun toiminnan teoria (TRA, Theory of Reasoned Action).

Mallien avulla pystytään ennustamaan ja selittämään käyttäjien hyväksyntää vahvalle tunnistautumiselle verkkokauppojen maksutoiminnassa. Davisin TAM-malli on näistä malleista tutkituin ja yleisin malli (Van Raaij & Schepers; 2008, Venkatesh, 2000), mutta se käsittelee organisaatiotasolla teknologian käyttöönottoa, joten tutkimukseen tarvitaan myös enemmän kuluttajien käyttäytymistä ennustava UTAUT-mallin toinen versio, joka on saanut paljon vaikutteita muun muassa TAM-mallista.

Taulukossa 1 on esitelty teknologian omaksumismallien kehitys perustellun toiminnan teoriasta (TRA) teknologian hyväksymisen ja käytön yhdistettyyn teoriaan (UTAUT2). Perustellun toiminnan teoria on teknologian hyväksymismallin perusta. Teknologian hyväksymisen ja käytön yhdistetty teoria UTAUT puolestaan perustuu sekä teknologian hyväksymismalliin, että perustellun toiminnan teoriaan, mutta näiden lisäksi myös muutamaan muuhun malliin, jotka ovat syntyneet näiden kahden lisäksi suositun tutkimuksen johdosta.

TAULUKKO 1 Teknologian omaksumismallien kehitys

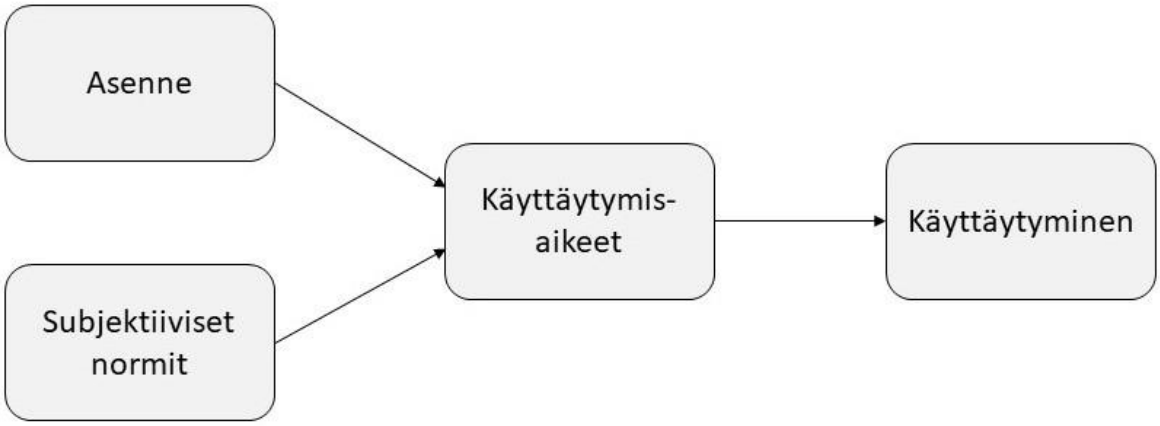
Teoria	Lyhenne	Kehittäjä(t)	Julkaisu-vuosi	Teorian pääkohdat
Perustellun toiminnan teoria	TRA	Ajzen & Fishbein	1980	Ennakoi ihmisen käyttäytymisen aikomusta subjektiivisten normien ja asenteen pohjalta.
Teknologian hyväksymismalli	TAM	Davis	1989	Käyttäjän teknologian käyttöaikomukseen vaikuttaa asenne sen käyttöön. Puolestaan asenteeseen vaikuttaa koettu hyödyllisyys ja koettu helppokäyttöisyys.
Yhdistetty teoria teknologian hyväksymisestä ja käytöstä	UTAUT	Venkatesh, Morris, Davis & Davis	2003	Teoria yhdistää aikaisemmat teknologian hyväksymismallit. Mallissa on neljä tekijää, suorituskyvyn odotukset, vaivannäön odotukset, sosiaalinen vaikutus ja helpottavat olosuhteet, jotka vaikuttavat teknologian käyttöaikomukseen ja teknologian käyttöön. Lisäksi mallissa on moderaattoreita, sukupuoli, ikä, kokemus ja käytön vapaaehtoisuus, jotka vaikuttavat näihin suhteisiin.
Yhdistetty teoria teknologian hyväksymisestä ja käytöstä	UTAUT2	Venkatesh, Thong & Xu	2012	UTAUT-teoriasta tehty toinen versio, missä edelliseen on lisätty kolme tekijää: koettu nautinto, hinta-arvo ja tottumus. Teoria on kehitetty tutkimaan kuluttajia organisaation työntekijöiden sijaan.

2.1 Perustellun toiminnan teoria

Perustellun toiminnan teoria TRA (Theory of Reasoned Action) on Fishbeinin ja Ajzenin kehittämä teoriamalli, joka ennakoi ihmisen käyttäytymistä subjektiivisten normien ja asenteen pohjalta (Fishbein ja Aizen, 1980; Fishbein, Ajzen ja Belief, 1975). Venkatesh (2000) sanoo teorian olevan yksi perustavanlaatuisista ja vaikutusvaltaisimmista teorioista, jotka käsittelevät ihmisen käyttäytymistä. Myös Rondan-Cataluña ym. (2015)

sanoo TRA:n olevan yleinen malli, jota on sovellettu monille eri aloille sen monikäyttöisyyden ansiosta. Kuviossa 1 on esitetty TRA-malli. Asenne ja subjektiiviset normit vaikuttavat ihmisen käyttäytymisaikeeseen, joka puolestaan johtaa käyttäytymiseen. (Ajzen & Fishbein, 1975).

Subjektiiviset normit tarkoittavat sosiaalista painetta, joka koostuu läheisten odotuksista ja käyttäjän motivaatiosta toteuttaa odotuksia. Käyttäjä voi kokea esimerkiksi muiden ihmisten hyväksymisestä tulevia paineita. (Park, 2000).



KUVIO 1 Perustellun toiminnan teoria (muokattu lähteestä Fishbein & Ajzen, 1975)

2.2 Teknologian hyväksymismalli

Edellä esitelty perustellun toiminnan teoria toimii pohjana teknologian hyväksymismallille TAMille. TAM oli ensimmäinen malli, jossa ihmisen psykologisia tekijöitä mainitaan tietokoneen hyväksymisen yhteydessä (Raaij ym., 2008). TAM perustuu TRAn muuttujien välisten suhteiden mallintamiseen. Siinä, kuten TRA:ssa, käyttö perustuu käyttöaikeeseen. (Rondan-Cataluña ym., 2015).

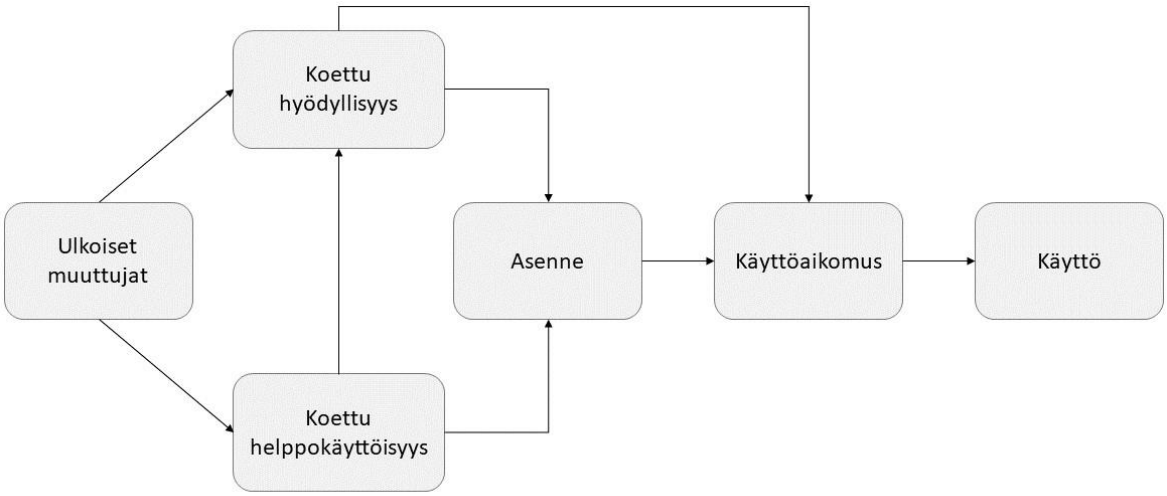
Kuviossa 2 on esitelty Davisin, Bagozzin ja Warshawin (1989) TAM-malli. Siinä on kaksi päätekijää: koettu hyödyllisyys (perceived usefulness) ja koettu helppokäyttöisyys (perceived ease of use). Näitä seuraa Asenne (attitude toward using). Siitä taas seuraa käyttöaikomus (behavioral intention to use), joka puolestaan johtaa lopulliseen teknologian käyttöön (actual system use). Kaaviossa on myös ulkoiset muuttujat (external variables), jotka vaikuttavat molempiin päätekijään. Ulkoisia muuttujia ovat esimerkiksi käyttäjän ja tehtävän ominaisuudet, toteutusprosessin luonne sekä organisaation rakenne. (Davis ym., 1989).

Davisin mukaan koettu helppokäyttöisyys tarkoittaa sitä, kuinka paljon käyttäjä uskoo tietyn järjestelmän olevan vaivatonta. Yleensä käyttäjä valitsee kahden sovelluksen väliltä sen, joka on helpompi käyttää. Koettu hyödyllisyys on hänen mukaansa käyttäjän uskomusta suorituksen parantamisesta. Käyttäjä siis arvioi, parantaako käytetty

teknologia työsuoritusta. (Davis, 1989). Asenteella tarkoitetaan tässä kaaviossa sitä, miten käyttäjä asennoituu teknologian käyttöön, eli se ei tarkoita tässä kaaviossa käyttäjän asennetta teknologiaa kohtaan vaan asennetta teknologian käyttöä kohtaan (Davis, 1985).

Koetun hyödyllisyyden ja koetun helppokäyttöisyyden välillä on yksisuuntainen suhde. Tämä tarkoittaa sitä, että käyttäjä yleensä ensin valitsee teknologian helppokäyttöisyyden mukaan ja vasta sen jälkeen hyödyllisyyden mukaan. Voidaankin sanoa, että koettu helppokäyttöisyys on erittäin tärkeässä roolissa, käyttäjän käyttäytymistä ennustettaessa. Asenne on koetun hyödyllisyyden ja koetun helppokäyttöisyyden summa, mitä enemmän käyttäjä kokee teknologian olevan helppokäyttöinen ja hyödyllinen, sitä positiivisempi hänen asenteensa on käyttää teknologiaa (Davis, 1985).

Davisin mallia on myöhemmin kehitetty siten, että siitä on poistettu asenne (Venkatesh & Davis, 1996). Tällöin TAM-malli auttaa ymmärtämään sitä, miten koettu hyödyllisyys ja koettu helppokäyttöisyys vaikuttavat käyttöaikomukseen. Se on selkeä lähestymistapa, jossa keskitytään kiinnostavaan avainriippuvuuteen. (Venkatesh, 2000).



KUVIO 2 TAM-malli. (Muokattu lähteestä Davis, Bagozzi & Warshaw, 1989)

TAM-mallia on käytetty alkuperäisesti tietokoneiden hyväksymisessä ja käyttöönotossa, mutta ajan myötä sitä on käytetty myös organisaatioissa eri teknologioiden käyttöönotossa. Siksi siitä on tullut yleinen ja vakiintunut hyväksymismalli. (Rondan-Cataluña ym., 2015). TAM-mallia on käytetty esimerkiksi sähköpostin hyväksymisessä, verkkokaupan aikeissa, oppilaiden verkko-oppimisessa (Hsu & Chang, 2013) sekä web-sivustosovelluksissa (Rondan-Cataluña ym., 2015).

TAM-mallista on laajennettu versiot TAM2 ja TAM3. Ensimmäisen laajennuksen eli TAM2:n on kehittänyt Venkatesh ja Davis vuonna 2000. Siinä koettu hyödyllisyys saa uusia erillisiä perusteita, mistä se koostuu. Perusteet voidaan jakaa kahteen kategoriaan: sosiaalisiin vaikuttamisprosesseihin ja kognitiivisiin instrumentaaliprosesseihin. Sosiaalisia vaikuttamisprosesseja ovat subjektiiviset normit, vapaaehtoisuus sekä mielikuva,

kun taas kognitiivisia instrumentaaliprosesseja ovat työn relevanssi, tulosten laatu, tulosten osoitettavuus ja koettu helppokäyttöisyys. (Rondan-Cataluña ym., 2015; Venkatesh ym., 2000). Lisäksi Rondan-C Cataluña ym. (2015) huomauttaa, että subjektiiviset normit vaikuttavat koetun hyödyllisyyden lisäksi myös suoraan käyttöaikomukseen.

TAM3-malli puolestaan laajentaa koettua helppokäyttöisyyttä. Helppokäyttöisyyden perusteet voidaan jakaa kahteen eri kategoriaan: inhimillisiin päätöksenteon ankkuroimiseen ja sopeutumiskehykseen. Inhimillisen päätöksenteon ankkurointiin kuuluu tietokoneen itsetehokkuus, tietokoneahdistus, tietokoneen leikkisyys ja ulkoisen ohjauksen käsitys. Sopeutumiskehykseen kuuluvat koettu nautinto ja objektiivinen käytettävyys. (Rondan-Cataluña ym., 2015).

2.3 Yhdistetty teoria teknologian hyväksymisestä ja käytöstä

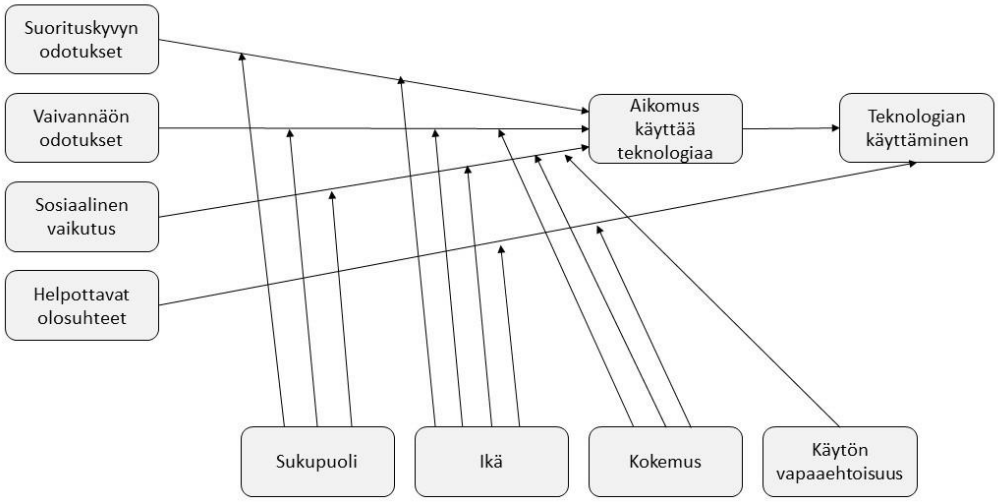
Yhdistetty teoria teknologian hyväksymisestä ja käytöstä eli UTAUT (Unified Theory of Acceptance and Use of Technology) on kehitetty 2000-luvun alussa, kun tietotekniikan lisääntyminen oli kiivaimmillaan ja täten myös tutkijat tutkivat aihetta paljon. Uusia malleja tuli paljon ja oikean mallin valitsemisesta tuli vaikeampaa. Niinpä Venkatesh ym. (2003) kehittivät UTAUT-mallin, joka on koottu kahdeksasta eri mallista. Nämä kahdeksan mallia ovat perustellun toiminnan teoria (TRA), teknologian hyväksymismalli (TAM), motivaatiomalli (MM), suunnitellun käyttäytymisen teoria (TPB), TAM:n ja TPB:n yhdistävä malli (C-TAM-TPB), PC:n käyttömalli (MPCU), innovaatioiden diffuusiteoria (IDT) ja sosiaalinen kognitiivinen teoria (SCT). (Venkatesh ym., 2003). Rondan-Cataluña ym. (2015) sanovat, että uuden teknologian käytön ja hyväksynnän selittämistä varten on luotu monia malleja sekoittaen eri teorioiden malleja luoden omaan tarkoitukseensa sopivan mallin. Juuri tämän takia yhdistetty teoria teknologian hyväksymisestä ja käytöstä on luotu, ettei tutkijoiden tarvitsisi luoda omaa räätälöityä mallia, vaan kaikki voisivat käyttää yhtä, tarpeeksi kattavaa mallia.

Kuvion 3 mukaan UTAUT-mallissa on neljä määräävää tekijää: suorituskyvyn odotukset, vaivannäön odotukset, sosiaalinen vaikutus ja helpottavat olosuhteet. Näistä helpottavat olosuhteet vaikuttavat suoraan teknologian käyttämiseen, kun taas kolme muuta, suorituskyvyn odotukset, vaivannäön odotukset ja sosiaalinen vaikutus vaikuttavat aikomukseen käyttää teknologiaa. (Venkatesh ym., 2003). Tämä siis poikkeaa hieman kahdesta aikaisemmasta esittelemästäni mallista TRA:sta ja TAM:sta siten, että teknologian käyttämiseen suoraan vaikuttavia tekijöitä onkin aikomuksen lisäksi myös helpottavat olosuhteet. (Rondan-Cataluña ym., 2015).

Suorituskyvyn odotukset tarkoittavat sitä, että kuinka hyödyllinen käyttäjä kokee teknologian olevan ja tuoko se tehokkuutta tai tuottavuutta tehtävän toteuttamiseksi. Vaivannäön odotukset ovat puolestaan järjestelmän helppokäyttöisyyttä ja opittavuutta. Sosiaaliset vaikutukset ovat läheisten (työnantajan, kavereiden tai perheen) antamia paineita teknologian käyttämisestä. Helpottavat olosuhteet ovat tietoja ja taitoja, joita vaaditaan teknologian käytössä tai tukevat sen käyttöä. (Venkatesh, 2003).

Kuviossa 3 on myös neljä avainmoderaattoria: sukupuoli, ikä, kokemus ja käytön vapaaehtoisuus. Ne moderoivat muiden tekijöiden suhteita. Tutkijat huomasivat jo vuonna 2003 tutkimusta tehdessä, että sukupuolen ja iän vaikutukset voivat kadota nuoremman sukupolven aikana, jotka ovat kasvaneet ja kouluttautuneet digitaaliajalla. (Venkatesh, 2003). Sukupuoli ja ikä siis vaikuttavat ajan myötä koko ajan vähemmän, koska teknologiset osaamiset, kuten älypuhelimen ja internetin käyttö lisääntyvät jatkuvasti

iästä ja sukupuolesta riippumatta. Tilastokeskuksen mukaan internettiä on käyttänyt suomalaisista 16–89 vuotiaista viimeisen kolmen kuukauden aikana 93 prosenttia ja älypuhelin on 88 prosentilla käytössä. Miesten ja naisten osuudet eroavat enimmillään yhden prosentin keskiarvosta, joten ainakaan käyttöprosenteissa ei ole juurikaan eroja iän tai sukupuolen suhteen. (SVT, 2021b). Puolestaan kokemuksella on paljon suurempi vaikutus teknologian käyttöaikomukseen ja käyttöön (Palau-Saumell, Forgas-coll, Sánchez-García & Robres, 2019).



KUVIO 3 Yhdistetty teoria teknologian hyväksymisestä ja käytöstä (muokattu lähteestä Venkatesh ym. 2003)

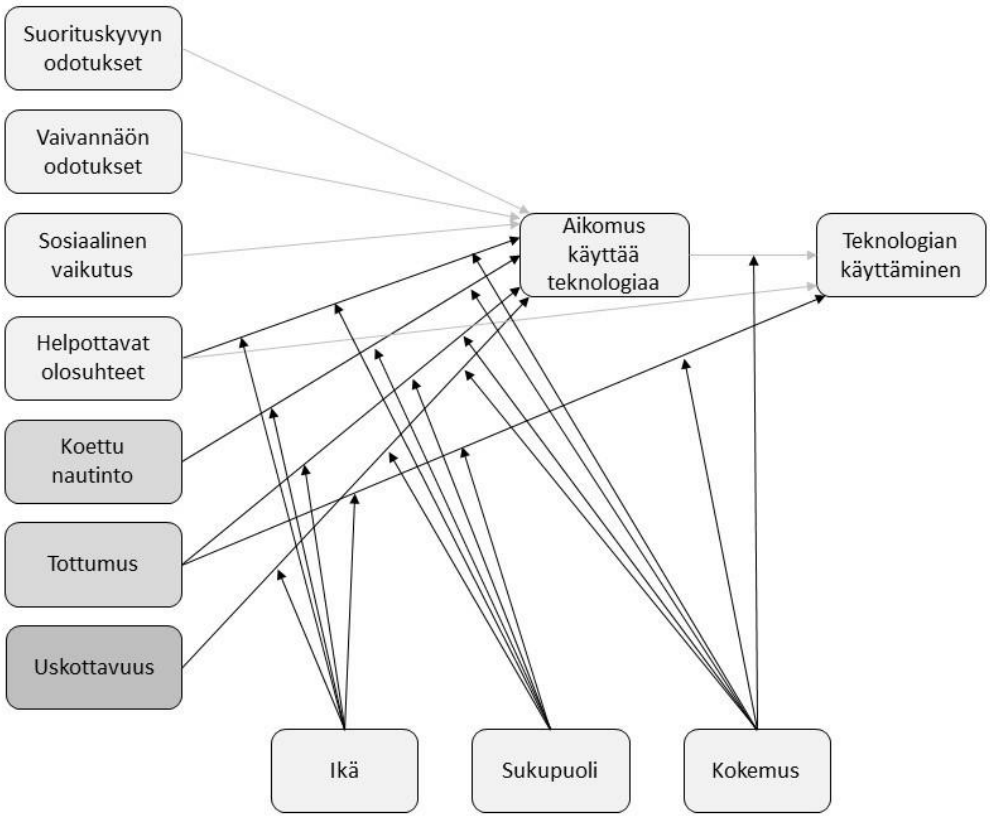
UTAUT-mallista on kehitetty toinen versio, UTAUT2-malli, joka on suunniteltu koskemaan enemmän kuluttajia kuin organisaatioita. Sen on kehitellyt Venkatesh, Thong ja Xu vuonna 2012. Kuviossa 4 on esitelty laajennettu UTAUT2-malli, jossa on pohjana UTAUT2-malli, mutta sitä on hieman muokattu tähän tutkielmaan sopivaksi. Muokkauksen idea tuli Palau-Saumellin ym. (2019) artikkelista. Palau-Saumell ym. (2019) esittivät UTAUT2-mallin laajennusta yhdellä lisätekijällä, joka on uskottavuus. Uskottavuus käsittelee käyttäjän uskomusta siitä, ettei teknologian käyttö aiheuta turvallisuus- eikä yksityisyysuhkia. (Palau-Saumell ym., 2019). Mallia muokattiin myös tähän tutkimukseen sopivaksi. Siihen lisättiin uskottavuus, koska vahva tunnistautuminen pyrkii parantamaan kuluttajien turvallisuutta ja täten uskottavuus on käyttöaikomuksen yksi määräävä tekijä. Lisäksi Palau-Saumell ym. (2019) muokkasivat hinta-arvoa säästämiseksi, kun heidän tutkimuksessaan teknologia ei maksanut kuluttajalle, vaan sen avulla pystyi säästämään rahaa. Tämän pohjalta tähän tutkimukseen tehtiin toinen muutos, hinta-arvon poistaminen, sillä vahva tunnistautuminen on kuluttajalle täysin ilmaista.

Kuviossa 4 on kuvattuna UTAUT2:n uudet suhteet tummilla nuolilla ja ensimmäisestä UTAUT-versiosta tutut suhteet ovat vaaleammilla viivoilla. Ensimmäisen version moderaattoreiden vaikutukset on jätetty kuviosta pois selkeyden vuoksi, mutta ne

kuuluvat siitä huolimatta myös uuteen malliin. Nämä moderaattoreiden vaikutukset voi tarkistaa kuviosta kolme.

Uusia tekijöitä UTAUT2-mallissa on uskottavuuden lisäksi koettu nautinto, hinta-arvo ja tottumus. Koettu nautinto on nimensä mukaan teknologian käytöstä saatavaa nautintoa. Siihen vaikuttavia moderaattoreita ovat ikä, sukupuoli ja kokemus. Hinta-arvo puolestaan tulee siitä, että UTAUT2 on kehitetty ennustamaan kuluttajien käyttäytymistä, kun edellinen versio oli organisaation käyttöympäristöön kehitetty. Organisaatioissa työntekijä ei joudu itse maksamaan teknologian käyttöönotosta, mutta kuluttajapuolella käyttäjän on itse maksettava teknologian käytöstä. Hinta-arvoon vaikuttavia moderaattoreita ovat ikä ja sukupuoli. Tämä kuitenkin poistettiin lopullisesta tutkimuksessa käytetystä mallista. Tottumus on aiempaa käyttäytymistä sekä sitä, kun käyttäjä uskoo käyttäytymisen olevan automaattista eli kun se on hänelle tapa. Tottumus on sekä teknologian käytön, että teknologian käyttöaikomuksen edeltäjä. Molempiin suhteisiin vaikuttavia moderaattoreita ovat kaikki kolme, ikä, sukupuoli ja kokemus. (Venkatesh ym., 2012).

UTAUT2-malliin on lisätty käyttöaikomuksen edeltäviin tekijöihin myös helpottavat olosuhteet. Se ei ollut ensimmäisessä versiossa, mutta uuteen versioon suhde on laitettu. Helpottavat olosuhteet tarkoittavat niitä resursseja, jotka käyttäjällä on käytettävissä. Toiseksi teknologian käyttöä edeltävän käyttöaikomuksen moderaattoriksi on lisätty kokemus. Viimeisenä eroavaisuutena ensimmäiseen versioon, uudessa mallissa on poistettu käytön vapaaehtoisuus -moderaattori. (Venkatesh ym., 2012).



KUVIO 4 UTAUT2 (muokattu lähteistä Venkatesh ym., 2012; Palau-Saumell ym., 2019)

2.4 Turvallisuus- ja yksityisyysuhat

Aikaisemmassa kappaleessa esittelin laajennetun UTAUT2-mallin, joka käsittelee yksittäisen kuluttajan teknologian hyväksymistä. Lisäsin malliin Palau-Saumellin ym. (2019) ehdottaman uskottavuuden, joka käsittelee turvallisuutta ja yksityisyyttä. Turvallisuus on suuri huolenaihe mobiilimaksujen keskuudessa (Wang, Shan, Chen, Zheng, Wang, Mingwei ja Haihua, 2020; Hammood, Abdullah, Hammood, Asmara, Al-Sharafi & Hasan, 2020). Tässä kappaleessa käyn läpi kirjallisuutta, joka käsittelee vahvan tunnistautumisen turvallisuus- ja yksityisyysuhkia.

Vahva tunnistautuminen on kehitetty parantamaan turvallisuutta ja poistamaan uhkia, joten turvallisuus- ja yksityisyysuhkia oli vaikeaa löytää. Koska vahvassa tunnistautumisessa käytetään hyvin usein matkapuhelinta, niin se on suurin turvallisuusuhka vahvassa tunnistautumisessa. Siihen liittyen löytyi myös melko hyvin tutkimuksia turvallisuus- ja yksityisyysuhista.

Mobiililaitteilla maksaminen eli mobiilimaksaminen on yksi verkkomaksamisen maksumenetelmä ja mobiilimaksaminen täyttää vahvan tunnistautumisen edellytykset. Wang ym. (2020) kertovat mobiilimaksamisen riskinä olevan sähköisen ja langattoman verkon käyttäminen. Mobiililaitteet voivat saada viruksia ja Wi-Fi-verkoissa tietojen todennus saatetaan siepata. Lisäksi mobiililaitteen varastamisen yhteydessä arkaluontoiset tiedot voivat päätyä rikollisten käsiin. Kunda & Chishimba (2018) sanovat, että haittaohjelmat, jotka hyökkääjä on esimerkiksi naamioinut toiseksi sovellukseksi, voivat kerätä käyttäjän syötteitä, kuten salasanoja, ja lähettää haittaohjelman keräämät tiedot hyökkääjän palvelimelle.

Hammood ym. (2020) puhuvat SIM-kortilla varmistamisesta vahvan tunnistautumisen yhteydessä. Se on erittäin varma käyttäjän todentamismenetelmä, mutta he löysivät siitä yhden uhan: SIM-kortin kloonaamisen. Vaikka kloonaaminen on todella hankalaa, niin löytyy ainakin yksi tapaus, missä kloonaaminen on toteutunut. Vuonna 2015 hakkerit saivat käsiinsä suuren SIM-korttivalmistajan salausavaimet, joilla hakkerit pystyvät valvoa puhe- ja viestiliikennettä. Hyökkäyksen kohteena oli Gemalto, joka valmistaa 2 miljardia SIM-korttia joka vuosi, 85:ssä eri maassa. (Scahill & Begley, 2015). Ylen tekemässä uutisessa aiheesta (Rigatelli, Pajunen & Orjala, 2015), Elisan Oy:n turvallisuusjohtaja Jaakko Wallenius on arvioinut, että hakkeroinnin vuoksi, yksittäisen käyttäjän SIM-kortti voidaan kloonata, mutta yksityisellä käyttäjällä ei ole vaaraa tulla hyökkäyksen uhriksi.

Vahvaan tunnistautumiseen käytetään nykyään paljon biometrisiä todentamismenetelmiä, kuten kasvo- tai sormenjälkitunnistusta. Ne eivät ole täysin turvallisia tunnistautumismenetelmiä. Esimerkiksi 3D-maskeilla voidaan päästä kasvojentunnistus läpi. (Galbally & Satta, 2016; Erdogmus & Marcel, 2014). Kasvontunnistusta kuitenkin käytetään pääsääntöisesti puhelimen sovelluksissa ja päästäkseen kokeilemaan 3D-maskia, rikollisen on aluksi saatava uhrin puhelin haltuunsa. Värillisten 3D-maskin tekeminen on kuitenkin vielä todella kallista, joten pieniin rikoksiin tätä ei kannata käyttää (Galbally ym., 2016). Erdogmusin ja Marcelin (2014) mukaan 3D-maskin tekeminen tulee koko ajan halvemmaksi ja näin myös kasvontunnistus tulee turvattomammaksi. Samaan aikaan kuitenkin laitteet kehittyvät ja ne pystyvät vaatimaan entistä tarkempia ja elävämpiä kasvoja tunnistautuessa. Nyt jo kasvontunnistus havaitsee silmänräpäytykset ja huulten liikkeet (Galbally ym., 2016). Todennusmenetelmät ovat turvallisia, mutta niitä täytyy kuitenkin jatkuvasti kehittää ja muuttaa, sillä hyökkääjät kehittävät myöskin heidän menetelmiään (Kunda ym., 2018).

Abbott & Patil (2020) tutkivat kaksivaiheisen tunnistautumisen (two-factor authentication) käyttöönottoa erään yliopiston henkilökunnalla ja opiskelijoilla. Kaksivaiheinen tunnistautuminen oli pakollista kaikissa yliopiston kirjautumistilanteissa. Yliopiston järjestelmään kirjautuessa se tuntui merkityksettömältä, mutta arkaluontoisten asioiden yhteydessä se koettiin hyödylliseksi. Tutkimuksessa he kuitenkin löysivät erään haavoittuvuuden. Älypuhelimen push-ilmoitukset, jotka tulevat näkyviin älypuhelimen yläreunaan automaattisina ilmoituksina, osoittautuivat suosituimmaksi ja vähiten turhauttaviksi todennusmenetelmiksi. Käyttäjät tottuivat käyttämään push-ilmoituksia kirjatumiseen siten, että enää ei tarkasti luettu ilmoitusta, vaan automaattisesti hyväksyttiin tapahtuma. Tämä mahdollistaa sen, että haitallinen push-ilmoitus voi hyvin toteutettuna mennä käyttäjän huomaamatta läpi.

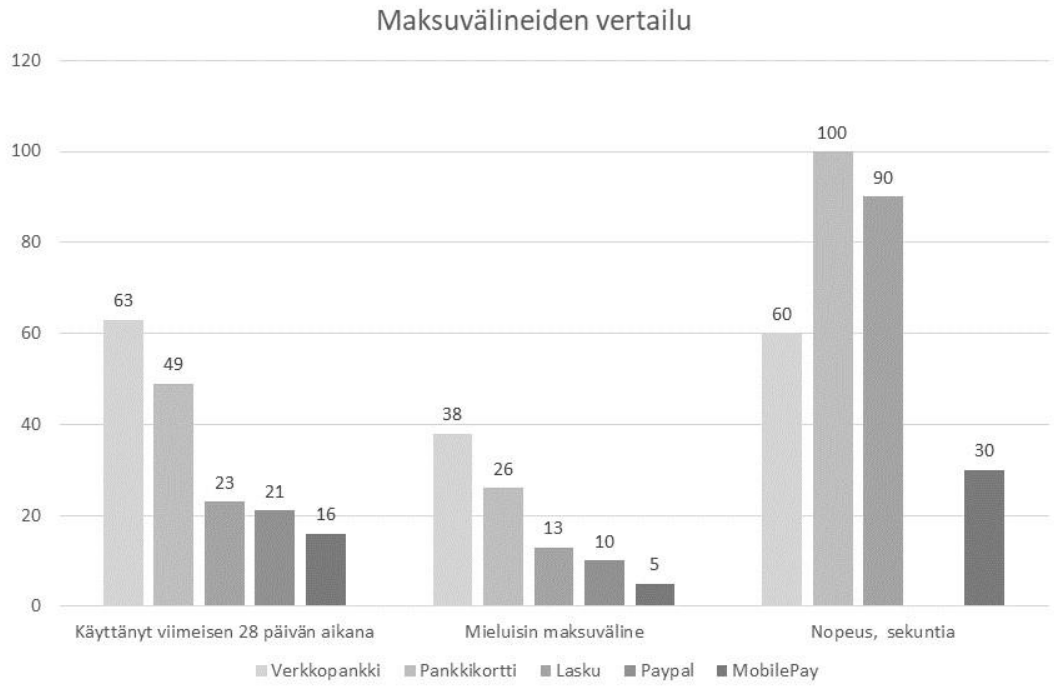
3 MAKSUVÄLINEET

Tässä luvussa selvitetään, mitä maksuvälineitä verkkokaupoilla on nyt, sekä miten ne toimivat ja eroavat toisistaan. Perinteisesti verkkokaupat ostavat maksupalvelut joltain palveluntarjoajalta kuten Paytraililta, Bluecommercelta, Klarnalta, Visma Paylta tai Stripeltä (Pyylampi, 2021). Ne ovat integroituja verkkokauppaan joko erillisinä integraatioina tai kaikki yhdellä integraatiolla siten, että käyttäjän tarvitsee painaa vain maksuvälineen logosta päästäkseen maksamaan ostoksensa (Alhonen, 2015). Perinteisiä maksuvälineitä ovat verkkopankki- ja pankkikorttimaksaminen sekä laskulla maksaminen. Uudempia ja vähemmän käytettyjä maksutapoja ovat erilaiset mobiilimaksut. Lopuksi esitellään vahvan tunnistautumisen välineitä ja niiden toimintaperiaatteita.

3.1 Maksuvälineet ja niiden yleisyys

Kuluttajilla on erilaisia maksuvälineitä verkko-ostojen maksamiseen. Suomessa neljä yleisintä maksuvälinettä ovat verkkopankkimaksu, pankkikorttimaksu, mobiilimaksaminen ja laskulla maksaminen. Yrityksen on kannattavaa tarjota useita erilaisia maksutapoja, jotta asiakas voisi maksaa ostoksensa verkossa haluamallaan tavalla (Alhonen, 2015 ja Huttunen, 2019). Wikholmin (2019) mukaan maksukanavia kannattaa olla vähintään kymmenen erilaista, sillä suppeammalla valikoimalla jotkut kaupoista voivat jäädä toteutumatta puuttuvan maksuvälineen vuoksi. Ostosten keskeytyksistä 8 % johtuu siitä, että haluttua maksutapavaihtoehtoa ei ollut verkkokaupassa saatavilla (Huttunen, 2019), joten työtä asian äärellä vielä riittää.

Perinteisiä maksutapoja kuluttajamarkkinoilla ovat pankkikorteilla ja verkkopankeilla maksaminen. Kuvion 5 kahdessa ensimmäisessä kategoriassa käydään läpi Paytrailin tilaama kyselyä, joka on Kantar ja Sifo -tutkimuslaitosten toteuttama. Siihen on vastannut 1546 suomaista kuluttajaa vuonna 2020. Paytrail on käyttänyt tutkimuksessaan myös omaa dataa, jota yrityksellä onkin melko paljon, sillä se hoitaa yli 10 000 verkkokaupan maksuliikennettä. (Borgström, Launo, Majaniemi, Oksanen & Tikkanen, 2020). Kuvion kolmannessa kategoriassa vertaillaan maksuvälineiden nopeuksia Karin (2020) mukaan.

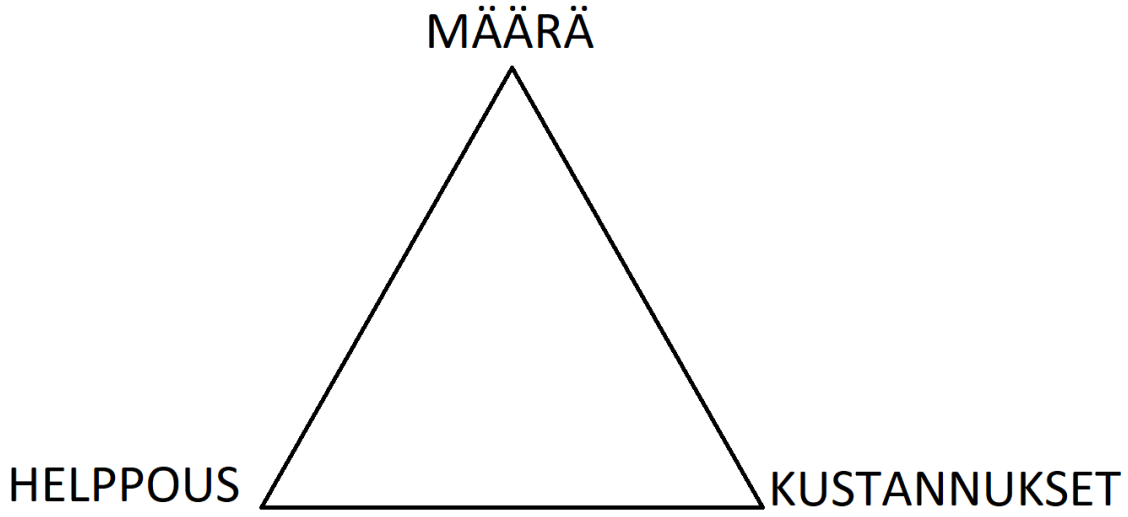


KUVIO 5 Maksuvälineiden vertailu (Muokattu lähteistä Borgström, Launo, Majaniemi, Oksanen & Tikkanen, 2020 ja Kari, 2020)

Tutkimuksen mukaan vuonna 2020 suomalaisista 63 % on käyttänyt verkkopankkimaksua viimeisen 28 päivän aikana. Kortilla maksaneita on 49 %. Näiden jälkeen seuraavaksi yleisin ja myös perinteinen maksutapa on laskulla maksaminen, jota on käyttänyt suomalaisista 23 % viimeisen 28 päivän aikana. Vähemmän yleisistä maksutavoista Paypalilla 21 % on tehnyt ostoja viimeisen 28 päivän aikana ja MobilePaylla 16 %. Samassa tutkimuksessa kysyttiin myös mieluisinta maksutapaa. Verkkopankkimaksu on vuonna 2020 mieluisin tapa 38 prosentille kuluttajista, korttimaksu 26 prosentille, lasku 13 prosentille, Paypal kymmenelle prosentille ja MobilePay viidelle prosentille. (Borgström, Launo, Majaniemi, Oksanen & Tikkanen, 2020). Jo seuraavana vuonna 2021 erääseen Paytrailin webinaariin osallistujilta kysyttiin, mikä maksutapa on mieluisin käytettävä. Mobiililompakolla maksaminen, johon MobilePay kuuluu, sai 53 prosenttia äänistä. Toiseksi suosituin oli verkkopankkimaksu 29 prosentilla ja kolmantena korttimaksu 18 prosentilla. Laskulla maksaminen ei ollut kenenkään mielestä mieluisin vaihtoehto. (Hakala, 2021). Tässä täytyy muistaa, että otanta on hyvin pieni eikä tulos ole yleistettävissä, mutta tämä antaa silti viitteitä siitä, mihin suuntaan ollaan menossa. Mobiilimaksamisen suosio on suuressa kasvussa sen helppokäyttöisyyden takia.

Voidaan myös pohtia, onko vahva tunnistautuminen ollut syy näin voimakkaaseen mobiilimaksamisen suosion kasvuun, sillä se on kaksi kertaa nopeampi maksutapa kuin verkkopankkimaksu ja yli kolme kertaa nopeampi kuin korttimaksu maksun kestojen mediaania katsottaessa (Kuvio 5; Kari, 2020). Vahva tunnistautuminen on hidastanut esimerkiksi pankkikortilla maksamista, koska tapahtuma täytyy erikseen vielä vahvistaa verkkopankkitunnuksilla. Mobiilimaksamisen suosion kasvu tapahtuu juuri vuonna 2021, jolloin maksupalveludirektiivi on Suomessa viimeisiltäkin osin otettu käyttöön.

Verkkokauppojen maksukanavien optimointi on tärkeää ajatella kuluttajien näkökulmasta katsottuna, mutta sitä on syytä tarkastella myös kauppiaan kustannusten kannalta. Wikholm (2019) esittelee maksukanavien optimoinnin kolmiometodiajattelun (kuvio 6), jossa kolme päätekijää maksukanavien valitsemiseen ovat maksukanavien määrä, helppous ja kustannukset. Kuvion 6 mukaan kaikki kolme päätekijää ovat yhtä suuressa roolissa. Maksukanavien määrän on oltava tarpeeksi suuri, mieluiten yli 10 kappaletta. Maksukanavan helppous on myös tärkeä, sillä suuri osa käyttäjistä valitsee maksuvälineen juuri sen helppouden takia. Myös kustannukset on otettava huomioon, koska maksuvälineiden kustannuksissa on suuria eroja. Myös Huttunen (2019) kehottaa huomioimaan maksuvaihtoehtojen erisuuruiset kustannukset.



KUVIO 6, Maksukanavien optimoinnin kolmioajattelu (Muokattu lähteestä Wikholm, 2019)

3.1.1 Verkkopankki

Verkkopankkimaksaminen on suomalaisten ylivoimaisesti käytetyin maksuväline (Hakala, 2021). Syy tälle on yksinkertainen, kuluttajat kokevat verkkopankkimaksamisen olevan tutuin maksuväline (Borgström ym., 2020).

Suomessa ainakin kymmenen eri pankkia tarjoavat pankkimaksuja palveluntarjoajien kautta. Ne ovat Nordea, Osuuspankki, Danske Bank, Säästöpankki, Oma Säästöpankki, POP Pankki, Aktia, Handelsbanken, Ålandsbanken ja S-Pankki. Verkkopankkimaksulla maksamisen prosessi etenee siten, että verkkokaupassa klikataan valitsemaa pankin logoa, jolloin istunto siirtyy pankin tunnistautumissivustolle, jossa käyttäjä kirjautuu sisään pankin antamilla tunnuksilla. Tämän jälkeen käyttäjä valitsee tilin, mistä maksu suoritetaan ja vahvistaa maksun. Istunto siirtyy automaattisesti takaisin verkkokauppaan maksun suoritettua.

3.1.2 Pankkikortti

Turvallisuus on verkko-ostamisessa ihmisten suurin ja tärkein huolenaihe (Bezoyski, 2016). Suomalaiset kokevat Paytrailin (2020) tuottaman tutkimuksen mukaan, että pankkikortilla maksaminen on turvallisin vaihtoehto verkkomaksuvälineistä (Borgström ym.,

2020). Pankkikortit jaetaan yleensä kahteen eri kategoriaan, luotto (credit) ja pankki (depit). Luottokortit ovat maailmanlaajuisesti yleisin maksuvaihtoehto kaikissa verkossa tapahtuvissa transaktioissa, mutta se on suosittu lähinnä yritysten välisessä kaupankäynnissä. (Bezoyski, 2016; Paunov & Vickery, 2006). Luottokorttitapahtumat ovat melko kalliita, joten ne eivät sovellu pienille yrityksille, eivätkä kuluttajille. Myös peruuntuneista luottokortilla tapahtuneista verkkomaksuista kustannukset jäävät yleensä kauppiaan maksettavaksi, jos heillä ei ole asiakkaan allekirjoitusta. Toistuvat peruuntuneista maksuista tulevat kustannukset voivat koitua liian kalliiksi pienille verkkokauppiaille, joten heidän ei välttämättä kannata tarjota sitä maksuvaihtoehtoa. (Paunov & Vickery, 2006).

Luottokortilla maksaminen tapahtuu välittäjän kautta. Luottokortin luovuttaja myöntää asiakkaalle luottoa, joka on asiakkaan käytössä. Luoton takaisin maksaminen tapahtuu esimerkiksi laskulla kerran kuukaudessa, mutta siihen laskutetaan lisäksi korko. Luottokortin myöntäjät antavat ostoksille lisäsuojan, joka korvaa esimerkiksi matkaliput, jos matkatoimisto menee konkurssiin ja matkatoimisto ei pysty itse korvaamaan peruuntuneen matkan lippuja takaisin (S-pankki, 2022).

Pankkikortit (debit) puolestaan ovat kuluttajien ja pienten yritysten suosiossa. Siinä maksu veloitetaan suoraan asiakkaan pankkitililtä, eikä välittäjän kautta niin kuin luottokortilla. Tällöin ostoksille ei yleensä saa mitään lisäsuojaa. (Paunov ym., 2006). Pankkikortilla maksaminen sopii mikromaksuihin, koska niihin ei yleensä tarvita lisäsuojaa (Bezoyski, 2016).

Nykyään monet verkkokaupat tarjoavat mahdollisuutta, jossa pankkikorttien tiedot pystytään täyttämään automaattisesti kuvasta (Raka, Agrwal, Kolhe, Karad, Pujeri, Thengade & Pujeri, 2019). Tämä nopeuttaa maksutapahtumaa ja se on nykyään myös siltä osin turvallista, että kortin tietojen lisäksi tarvitsee vahvan tunnistautumisen Euroopan unionin alueella tapahtuvissa verkkomaksuissa.

3.1.3 Mobiilimaksaminen

Suomessa yleisin mobiilimaksamisen sovellus on MobilePay. Muita sovelluksia ovat muun muassa Pivo, Siirto, Apple Pay ja Google Pay. Mobiilimaksamisen suosio on koko ajan kasvava. (Sintonen ym., 2021). Mobiililaitteista on tullut yksi kaikkien aikojen merkittävimmistä kuluttajille suunnatuista tuotteista. Mobiililaitteiden laaja palveluvalikoima ja arvon luominen monessa ulottuvuudessa on merkittävin syy sille, miksi mobiililaitteesta on tullut niin tärkeä laite kuluttajille. (Aydin & Burnaz, 2016). Yksi mobiililaitteen ulottuvuus on maksaminen. Kun kuluttajat kantavat mobiililaitetta nykyään mukanaan lähes kaikkialla, sillä on helppoa ja nopeaa toteuttaa monia arjen tehtäviä, kuten verkkoostoja.

Mobiilimaksaminen edellytyksenä on, että käyttäjällä on avattuna pankkitili ja pankkikortti, joilta maksu välitetään kauppiaalle (Kang, 2018). Lisättyäsi pankkikortin mobiilisovellukseen, voit tehdä maksuja muun muassa verkkokaupoissa. Verkkokaupan kassalla valitset maksuvälineeksi esimerkiksi MobilePayn, jos sellainen on verkkokaupan maksuvälineiden vaihtoehdoissa. Jos teet ostoksia puhelimella, niin puhelin avaa automaattisesti sovelluksen puhelimessasi. Sitten täytyy vain kirjautua sisään joko salasanalla tai biometrisellä tunnisteella kuten sormenjäljellä tai kasvontunnistamisella. Tietokoneella maksaessa, täytyy syöttää puhelinnumero, jolla maksu suoritetaan ja avata puhelimesta mobiilimaksusovellus. Lopuksi täytyy hyväksyä maksu pyyhkäisemällä näytöllä olevasta kohteesta. Aikaa tähän kuluu noin puoli minuuttia. Mobiilimaksamisen etuna muihin maksuvälineisiin onkin juuri palvelun nopeus ja helppous (Borgström ym., 2020).

Hoofnagle, Urban & Li tutkivat ja pohtivat jo vuonna 2012 mobiilimaksujärjestelmien mahdollisuuksia. Heidän mukaansa mobiilimaksaminen tulee alentamaan transaktiomaksuja ja lisäävät käyttömukavuutta. Käyttömukavuus tulee esiin muun muassa kuluttajien helpon tunnistautumisen kautta ja ostotietojen jakamista useille yrityksille. Tämä on juuri sitä, mitä mobiilimaksaminen ja mobiililompakot ovat nykyään. Mobiililompakoiden yksi hyöty on myös se, että lompakkoa voidaan käyttää niin pankkikorttien kuin kuittienkin varastoina. Sinne voidaan tallentaa käyttäjien kuitteja ja takuutodistuksia, jotka ennen ovat olleet vaarana hukkua tai kulua niin, ettei tekstistä saa selvää. Tämä voi osittain ratkaista takuupalautuksien hylkäämisen ongelman. (Hoofnagle ym., 2012). Nykyään esimerkiksi S-ryhmällä on käytössään sähköinen kuittipalvelu, mihin saa kaikki kuitit talteen, jos käyttää S-etukorttia maksaessa.

3.1.4 Lasku ja PayPal

Laskulla maksaminen on hyvin perinteinen maksumuoto verkkomaksuissa. Siinä ostokset maksetaan myöhemmin, asiakkaalle lähetettävällä laskulla. Monet yritykset tarjoavat myös osamaksupalvelua, jolloin isommat ostokset voidaan jakaa useammalle laskulle. Jotkut tarjoavat tätä nollakorolla, mutta yleensä maksuajasta peritään pientä korkoa.

Suomessa verkko-ostojen maksaminen laskulla ei ole kovin yleistä, mutta esimerkiksi Suomen naapurimaassa Ruotsissa laskulla maksaminen on mieluisin maksuvaihtoehto vuonna 2020. (Borgström ym., 2020).

PayPal koetaan turvallisena sekä kuluttajille, että kauppiaille. Tämän lisäksi se on myös nopea maksutapa, missä ei tarvitse syöttää monia eri tietoja vaan sähköpostiosoitteella kirjautuminen riittää. PayPal on maailmanlaajuisesti suosituin maksuväline, mutta suomessa sitä pitää mieluisimpana vain 10 % väestöstä. (Niranjanamurthy, 2014; Borgström ym., 2020). PayPal on myös kauppiaan kannalta helppo, nopea ja halpa tapa tarjota maksupalvelua verkkosivuillaan. Se ei tarvitse erikseen mitään kallista palveluntarjoajaa, vaan sen voi lisätä ilman aloitusmaksua verkkokauppaan. (Niranjanamurthy, 2014; Pyylampi, 2021).

4 MAKSUPALVELUDIREKTIIVI

Tässä luvussa ensiksi käsitellään PSD2 maksupalveludirektiiviä ja sen voimaan saattamista. Direktiivi käsitteenä on Euroopan unionin määrittelemä tavoite, johon kaikkien Euroopan unionissa olevien valtioiden täytyy yltää. Euroopan unioni ei kuitenkaan itse määrää jäsenvaltioidensa lakeja direktiiveillä, vaan jäsenvaltiot voivat itse määritellä lakinsa siten, että direktiivin tavoite täyttyy. (Euroopan unioni, 2022). Tämän jälkeen luvussa käsitellään direktiivin keskeisimpiä muutoksia, joita ovat kolmansien osapuolien tuominen sääntelyn piiriin sekä vahvan tunnistamisen tuominen verkkomaksuihin. Kolmanneksi käsittelemme tutkimuksen kannalta tärkeintä maksupalveludirektiivin muutosta vahvaa tunnistamista.

4.1 Direktiivin tavoite ja voimaan saattaminen

Euroopan komissio ilmoitti lehdistötiedotteessaan vuonna 2015, että Euroopan parlamentti on hyväksynyt uuden direktiivin, jota komissio on ehdottanut vuonna 2013 Euroopan parlamentille. Maksupalveludirektiivin (PSD2) tarkoituksena on tarjota kaikille eurooppalaisille kuluttajille turvallista ja helppoa maksamista verkossa niin maan sisällä kuin muissa Euroopan unionin jäsenvaltioissa. (European Comission, 2015). Sen tarkoituksena on siis maksupalveluiden kehittäminen Euroopan unionissa (Wolters ja Jacobs, 2019). Wolter ym. (2019) korostaa, että tavoitteena on käyttäjäystävällisten maksutapojen kehittäminen. Vahvan tunnistautumisen myötä nopeat ja helpot maksuvälineissä toimivat tunnistautumiset tulevat yleistymään ja täten myös edistämään tätä tavoitetta.

Vahvan tunnistamisen voimaan saattaminen toteutetaan jokaisessa Euroopan unionin jäsenvaltiossa oman lain muokkaamisella direktiivin ehdot täyttäviksi. Suomessa laki tuli voimaan kahdessa eri osassa, koska Euroopan pankkiviranomainen (EBA) antoi lisäaikaa verkkokaupan pankkikorttimaksamisen vaatimuksille. Vahvaa tunnistamista koskeva sääntely on tullut voimaan 14.9.2019, mutta korttimaksuissa lisäaikaa on annettu 31.12.2020 saakka, jolloin muutosprosessi täytyy olla toteutettuna kokonaisuudessaan. (Finanssivalvonta, 2019b). Verkkokauppojen ja maksupalveluntarjoajien on tunnistettava asiakas vahvalla tunnistamisella 1.1.2021 alkaen.

4.2 Keskeiset muutokset

Euroopan unionin PSD2-direktiivin suurimmat muutokset koskevat maksupalveluntarjoajien kolmansia osapuolia (Third Party Payment Service Provider, TPP), jotka eivät aikaisemmin ole kuuluneet maksupalvelulainsäädännön piiriin. Kolmansia osapuolia, jotka tulevat nyt sääntelyn piiriin ovat maksutoimeksiantopalvelun tarjoajat (Payment Initiation Service Providers, PISP) ja tilitietopalvelun tarjoajat (Account Information Service Providers, AISP). Lyhyesti sanottuna uudistuksen jälkeen näillä kyseisillä kolmansilla osapuolilla on pääsy asiakkaan tilille, jos asiakas on siihen suostunut. (Finanssivalvonta, 2019c). Esimerkiksi tilitietopalvelu voi yhdistää monia eri pankkitilejä ja muodostaa kuluttajalle kulutustottumuksistaan raportin, josta käyttäjän on itse helppo analysoida omaa kulutustaan. Maksutoimeksiantopalvelun tarjoajat auttavat maksun käynnistämistä muodostamalla niin sanotun ”sillan” asiakastilin ja kauppiaan tilin välille. Tämän odotetaan tuova uusia kilpailijoita markkinoille ja maksut tulevat halvemmiksi Euroopassa. (Możdżyński, 2017).

Tämän tutkielman keskeisin aihe direktiivin muutoksissa on vahvan tunnistautumisen vaatimus sähköisissä maksutapahtumissa. Vahvaa tunnistautumista on käytetty jo aikaisemmin muun muassa verkkopankkimaksuissa. Direktiivi koskeekin pääsääntöisesti pankkikorttimaksujen uudistamista siten, että pelkästään pankkikorttien tiedoilla ei pysty tekemään Euroopan unionin alueella verkko-ostoja, vaan siihen vaaditaan maksaessa käytetyn pankkikortin haltijan tunnistus kyseisen pankin tunnistusmenetelmillä, joita ovat esimerkiksi tunnuslukusovellus ja tunnuslukulaite. Verkkokaupasta mobiilimaksulla maksaessa vahva tunnistautuminen tulee myös automaattisesti, koska maksaminen tapahtuu käyttäjän matkapuhelimessa olevan sovelluksen avulla. Vahvan tunnistautumisen todennustekijät esitellään luvussa 4.3.

Jokainen Euroopan unionin jäsen valtio määrittää omassa laissaan tarkemmat lait, miten vahva tunnistaminen toteutetaan. Tässä kappaleessa on suorat viittaukset Suomen lainsäädäntöön ja EU:n direktiiviin:

Suomen lainsäädännössä laki 898/2017, 85 b § ilmoittaa, että (Finlex, 2017)

> Palveluntarjoaja on käytettävä vahvaa tunnistamista, jos maksaja
> 1) käyttää maksutiliään tietoverkon välityksellä;
> 2) käynnistää sähköisen maksutapahtuman;
> 3) toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski.

Nämä ovat samat kolme kohtaa, jotka EU määrittelee direktiivissä 2015/2366 artiklassa 97, jotka jäsenvaltioiden on täytettävä omissa laissaan. Tämän lisäksi:

> ”Jäsenvaltioiden on varmistettava, että maksupalveluntarjoajat ovat ottaneet käyttöön riittäviä turvatoimenpiteitä suojatakseen maksupalvelunkäyttäjien henkilökohtaisten turvatunnuksien luottamuksellisuuden ja eheyden. ”

Direktiivin 2015/2366, artiklassa 98 kerrotaan poikkeuksista seuraavasti (Euroopan unioni, 2015):

Poikkeusten on perustuttava seuraaviin perusteisiin:
a) tarjottuun palveluun liittyvän riskin taso;
b) maksutapahtumien määrä, toistuvuus tai molemmat;
c) maksutapahtuman toteuttamiseen käytetty maksukanava.

4.3 Vahva tunnistaminen ja vahva tunnistautuminen

Tässä luvussa kerron, miten vahva tunnistautuminen eroaa vahvasta tunnistamisesta. Sitten kerron mitkä ovat vahvan tunnistautumisen vaatimukset ja lopuksi käyn läpi erilaisia vahvan tunnistautumisen menetelmiä.

Vahva tunnistaminen on käyttäjän tunnistamista eli oikean henkilön todentamista verkossa tapahtuvassa tiedon käsittelyssä (Hammood ym., 2020; Fabcic, 2020). Vahva tunnistautuminen on puolestaan henkilön puolesta tapahtuva tunnistautumistapahtuma. Tunnistautuminen edistää kyberturvallisuutta (Fabcic, 2020). Perinteisesti vahvaa tunnistautumista on käytetty kirjautuessa verkkopankkiin, mutta muun muassa verkkokauppojen yleistyttyä sitä on alettu käyttämään myös asiakkaan henkilöllisyyden todentamisessa.

Tunnistautuminen on heikkoa tunnistautumista silloin, kun käytössä on pelkästään käyttäjätunnus ja salasana tai esimerkiksi pankkikortin tiedot. Kun salasanan ja käyttäjätunnuksen lisäksi kirjautumiseen vaaditaan käyttäjän hallussa olevan esineen käyttö (yleensä matkapuhelin) tai biometrinen tekijä, tunnistautumisesta tulee vahva tunnistautuminen. Suomen laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617 §8a) kerrotaan, että tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä:

1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedoissaan;
2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;
3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.

Kohdan yksi todentamistekijä voi olla esimerkiksi käyttäjätunnus ja salasana tai PIN-koodi, kohdan kaksi todentamistekijä voi olla esimerkiksi puhelin tai tunnuslukukortti ja kohdan kolme todentamistekijänä voi toimia käyttäjän sormenjälki tai kasvontunnistus (Finanssivalvonta, 2019b).

4.3.1 Pankkitunnukset

Pankkitunnukset ovat kunkin pankin omia tunnistusvälineitä asiakkailleen. Pankkitunnukset ovat henkilökohtaisia ja niitä voidaan käyttää niin pankin verkkopalveluihin kirjautumiseen kuin myös muiden palveluiden sähköiseen tunnistautumiseen. (Suomi.fi, 2022). Pankkitunnukset ovat yleisin tunnistautumisväline Suomessa.

Pankkitunnusten tunnistautuminen käytti ennen suomalaisten pankkien luomaa TUPAS-protokollaa tunnistautumisessa, mutta se korvattiin vuonna 2019 uudella protokollalla, joka on turvallisempi kuin aikaisempi. Pankkitunnistusta käyttävien oli vaidettava 1.10.2019 mennessä TUPAS-protokollan tilalle kansainvälisistä protokollista OpenID Connect tai SAML. Protokollan vaihtaminen ei näkynyt loppukäyttäjille millään tavalla, vaan se on palveluntarjoajien muutosprosessi. (Kyberturvakeskus, 2021). Nämä ovat siis kansainvälisesti luotettuja kehyksiä, jotka välittävät käyttäjien todennus- ja käyttöoikeustietoja (Naik ja Jenkins, 2017).

Suomen julkishallinnon organisaatioiden ei tarvitse käyttää OpenID Connect- tai SAML-protokollaa, sillä niiden verkkopalvelut käyttävät vahvan tunnistautumisen tarjoamisessa Suomi.fi-palvelua, joka on kehitetty pelkästään suomalaisten julkishallinnon organisaatioiden käyttöön, esimerkiksi Kelan tai verottajan palveluiden verkkosivuille kirjautumiseen. (Suomi.fi, 2022).

4.3.2 Mobiilivarmenne

Mobiilivarmenne toimii suomalaisten matkapuhelinoperaattoreiden tarjoamilla SIM-korteilla siten, että käyttäjä aktivoi operaattorin kanssa SIM-kortille mobiilitunnistautumisen. Suomessa mobiilivarmennetta tarjoavia operaattoreita ovat Telia, Elisa ja DNA. Mobiilivarmenne toimii matkapuhelimen välityksellä, kun SIM-kortti on asennettuna kyseiseen matkapuhelimeen. Palvelun aktivointi tapahtuu oman SIM-kortin operaattorin kanssa ja aktivoinnin yhteydessä käyttäjä valitsee itselleen tunnusluvun, jonka hän syöttää käyttäessään mobiilivarmennetta tunnistautumiseen. Mobiilivarmenne on pankkitunnuksiin verrattava tunnistautumisväline. (Mobiilivarmenne.fi, 2022; Suomi.fi, 2022).

Mobiilivarmennetta ei voida käyttää verkko-ostojen maksamisen vahvassa tunnistautumisessa, mutta sen käyttökohteita ovat kirjautumiset yksityisiin tai julkisiin verkkopalveluihin.

4.3.3 Biometrinen tunnistautuminen

Käytössä olevia biometrisiä todennustekniikoita ovat kasvontunnistus, sormenjälki, äänentunnistus ja iiriksen seuranta. Biometrisen tunnistautumisen etuja ovat sen nopea todentaminen sekä vaikeus käsitellä ja murtaa. Lisäksi se on helpompi muistaa ja kantaa mukana, koska tunnisteet kulkevat itsekseen aina käyttäjän mukana. Toisin kuin hyvän salasanan muistaminen on vaikeaa ja puolestaan helposti muistettavan salasanan murtaminen on todella helppoa. (Gupta, Agarwal & Sivakumar, 2020; Kunda ym., 2018). Biometrinen tunnistautumisen todennus toimii siten, että sormenjälki tallennetaan laitteelle matemaattisesti ja sitä verrataan aina siihen sormenjälkeen, joka saadaan jonkun yrittäessä lukituksen avausta. (Gupta, Agarwal & Sivakumar, 2020). Matemaattinen tallennus tarkoittaa sitä, että kuvaa sormenjäljestä tai kasvoista ei tallenneta kuvana, vaan niin sanottuna tiivisteenä kuvasta. Mikko Hyppönen kertoo kirjassaan Internet (Hyppönen, 2021), että Iphoneissa sormenjäljestä ja kasvontunnistusksesta ei lähetetä tietoja Applelle, vaan niistä tehdään yksisuuntainen tiiviste, joka tallennetaan puhelimen turvapiiriin. Tiivisteestä ei pysty mitenkään luomaan alkuperäistä sormenjälkeä tai kasvontietoja, joten se on todella turvallinen salausmenetelmä.

4.3.4 Muut tunnistautumismenetelmät

Yllä esiteltyjen tunnistautumismenetelmien lisäksi on olemassa muitakin tunnistautumismenetelmiä, jotka ovat pääsääntöisesti älypuhelinsovelluksia, kuten Google Authenticator (Abbott & Patil, 2020). Näissä sovelluksissa tunnistautumisen toinen vaihe tehdään puhelimen sovelluksessa, jossa joko syötetään käyttäjän valitsema koodi tai käydään hakemassa jokin koodi, joka sitten liitetään kirjautumissivustolla olevaan kenttään. Esimerkiksi Google Authenticator toimii niin sanotulla kertakäyttöisellä salasanalla (one-time password), joka on kuusinumeroinen koodi ja se vaihtuu 30 sekunnin välein.

Toinen esimerkki kertakäyttöisestä salasanasta on tekstiviestillä lähetettävä kertakäyttöinen salasana. Siinä käyttäjä syöttää puhelinnumeronsa verkkosivuilla olevaan kenttään, jolloin järjestelmä lähettää ainutkertaisen koodin siihen puhelinnumeroon. Käyttäjä syöttää koodin sivulla ja näin vahva tunnistautuminen on toteutunut, kun puhelinta on käytetty tunnusten lisäksi. (Hammood ym., 2020). Muita tunnistautumismenetelmiä ei yleisesti käytetä verkkokaupassa maksamisen vahvistamiseen, vaan näiden käyttökohteita ovat mobiilivarmenteen tavoin kirjautumisen yhteydessä tapahtuva vahva tunnistautuminen.

5 TUTKIMUSMENETELMÄ

Tutkielman empiirinen osuus toteutettiin laadullisena eli kvalitatiivisena tutkimuksena. Tutkimusaihe liittyy ihmisen kokemuksen ymmärtämiseen ja tutkimiseen teknologian hyväksymisessä. Kvalitatiivisen tutkimuksen tavoitteena onkin käsitellä sellaisia kysymyksiä, jotka liittyvät kokemuksen ymmärtämiseen (Fossey, Harvey, McDermott & Davidson, 2002). Tämä tutkimus pyrkii vastaamaan tutkimuskysymyksiin

- Miten kuluttajat ovat kokeneet vahvan tunnistautumisen käyttöönoton?
- Miten vahvan tunnistautumisen on koettu vaikuttavan maksukäyttäytymiseen?

Aineisto kerättiin yksilöhaastatteluna puolistrukturoidulla menetelmällä. Haastateltavien kokemuksia ja tulkintoja aiheesta saa parhaiten kerättyä haastattelemalla (Puusa, Juuti & Aaltio, 2020). Tässä tutkimuksessa aiheena on vahvan tunnistautumisen kokemus ja verkkokaupan maksukäyttäytymisen muutoksen kokeminen. Puolistrukturoitu menetelmä on siksi hyvä menetelmä tähän tutkimukseen, että samalla haastattelurungolla voi vertailla eri haastateltavien kokemuksia, mutta samaan aikaan voi kysyä myös tarkentavia kysymyksiä kokemuksista. Toinen vaihtoehto menetelmäksi olisi ollut teemahaastattelu, mutta tässä tutkimuksessa haluttiin kokemuksia ennalta määrätyistä aiheista, joten tutkimuksessa ei ole tarkoitus antaa haastateltaville suuria vapauksia, kuten teemahaastatteluissa on tapana. (Saaranen-Kauppinen & Puusniekka, 2006). Täten puolistrukturoitu menetelmä sopii teemahaastattelua paremmin.

Haastateltaviksi valittiin kahdeksan nuorta aikuista kuluttajaa, jotka ovat tehneet ostoksia verkkokaupoissa ja ovat käyttäneet joskus korttimaksamista yhtenä vaihtoehtona. Ensimmäinen haastattelu toimi koehaastatteluna, joka sisällytettiin tutkimuksen tuloksiin, koska haastateltavan kokemukset nähtiin sopivan tähän tutkimukseen.

Haastatteluiden jälkeen aineisto litteroitiin ja teemoiteltiin. Litteroitua tekstiä tuli 31 sivua ja teemoittelu tehtiin Excel-taulukkoon. Teemoittelu oli pääosin teoriapohjainen ja perustui tutkimuksen teoriaviitekehyksenä käytettyihin UTAUT2-malliin ja TAM-malliin. Teemat on otettu UTAUT2-mallista teknologian käyttöaikomuksen määräävistä tekijöistä sekä TAM-mallista. UTAUT2-mallin vaivannäön odotuksiin ja suorituskyvyn odotuksiin on yhdistetty TAM-mallin helppokäyttöisyys ja hyödyllisyys, sillä ne käsittelevät samoja teemoja. TAM-mallista on otettu näiden lisäksi myös asenne yhdeksi teemaksi mukaan.

Tämän jälkeen aineisto analysoitiin. Kokemusten kartoittamiseen fenomenografinen analyysi on hyvä menetelmä. Saaranen-Kauppinen ja Puusniekka (2006) kertovat, että fenomenografisen analyysin tavoitteena on löytää eroavaisuuksia haastateltavien kokemuksista. Siinä käytetään kaksitasoista analyysia: Ensimmäisen tason tarkoituksena on löytää haastateltavien eri tulkinnat ja ymmärrykset tutkittavasta aiheesta, eli vahvasta tunnistautumisesta. Toinen taso puolestaan menee hieman aiheessa syvemmälle ja sen tarkoituksena on löytää syvällisiä merkityssisältöjä ja kokemuksia tutkittavasta aiheesta. (Saaranen-Kauppinen & Puusniekka 2006).

5.1 Haastateltavien rajaus

Haastateltavat rajataan sen perusteella, ketkä ovat tehneet verkkokaupan ostoksia vähintään 10 kertaa vahvan tunnistautumisen tultua osaksi verkkomaksamista. Lisäksi heillä on oltava vähintään saman verran ostotapahtumia ennen vahvan tunnistamisen tulemista verkko-ostoihin. Nämä ovat välttämättömiä vaatimuksia, sillä kokemusta täytyy olla sekä ennen että jälkeen, jotta saadaan mahdollisimman validia ja asiantuntevaa kokemusta tutkimukseen.

Tilastokeskuksen tietojen mukaan verkosta ostoja tekeviä on 16-vuotiaista aina 54-vuotiaisiin saakka yli 70 % väestöstä. Seuraavassa ikäluokassa lukema romahtaa reilusti alle 50 prosenttiin ja lopulta 11 prosenttiin 75–89-vuotiailla (SVT, 2021b). Rajaus on täten selkeä tehdä alle 54 vuotiaisiin, koska 16—54-vuotiaat tekevät huomattavasti enemmän verkko-ostoja muihin ikäryhmiin verrattuna. Rajasin kuitenkin ikäryhmää vielä lisää, nuoriin aikuisiin, koska toinen tutkimuskysymys ”miten vahvan tunnistautumisen on koettu vaikuttavan maksukäyttäytymiseen?” koskee maksukäyttäytymisen muutosta ja nuorten keskuudessa on eniten kiinnostusta uusista teknologioista (Wood, 2013)

Haastatteluun kysyttiin sellaisia kuluttajia, joilla pankkikortilla maksaminen oli joskus ollut tai oli sillä hetkellä mieluisin tai vähintään useasti käytössä ollut maksuväline. Tämä rajaus tuli ensimmäisen koehaastattelun jälkeen, kun haastattelun aikana tuli ilmi, että ilman kokemusta pankkikorttimaksamisesta ei haastattelusta saa tarvittavaa aineistoa, koska maksupalveludirektiivin säädös vahvasta tunnistautumisesta on muuttanut pelkästään pankkikorttimaksamista verkko-ostoissa. Seuraavia haastateltavia kysyttiin mukaan haastatteluun seuraavalla viestillä:

> ”Hei, onko pankkikortilla maksaminen verkkokaupoissa ollut aikaisemmin tai onko se nyt mieluisin maksuväline? Teen gradututkielmaa vahvan tunnistautumisen omaksumisesta verkko-ostoissa. Haluatko osallistua noin 30 minuutin haastatteluun, jossa kyselen sinun kokemuksia maksukäyttäytymisestäsi ja vahvan tunnistautumisen omaksumisesta?”

Viesti laitettiin kymmenelle henkilölle ja kuusi vastasi myöntyvästi, kolme ei vastannut lainkaan. Kutsutut olivat Jyväskylän yliopiston opiskelijoita eri tieteenaloilta tai lumipallomenetelmällä edellisistä haastatteluista saatuja. Yksi haastateltava tulki yliopiston ruokalan ruokapöytäkeskusteluista. Hänelle ei lähetetty kutsuviestiä haastatteluun, vaan hänen kanssaan sovittiin haastattelun ajankohta suullisesti.

5.2 Puolistrukturoidun haastattelun suunnittelu ja toteutus

Haastattelun suunnittelussa painotettiin käyttäjän kokemusta vahvan tunnistautumisen hyväksymisestä. Kysymykset muotoiltiin siten, että juuri heidän kokemuksensa tulisi esille. Haastattelun alussa kyseltiin teknologiaosaamisesta ja verkkokaupan käyttämisen maksutavoista. Nämä toimivat haastateltavien lämmittämisenä ja ne johdattivat haastateltavat kätevästi aiheen sisälle. Tämä toimi todella hyvin, sillä tämän osion jälkeen haastateltava oli asian ytimessä ja heiltä sai hyvää sisältöä vahvan tunnistautumisen kokemuksesta. Haastattelun runko on liitteenä (LIITE 1).

Toinen osio, vahvan tunnistautumisen kokemus, suunniteltiin siten, että se pohjautuu teoriaviitekehykseen, muokattuun UTAUT2-malliin. Kysymykset pohjautuivat mallissa olevan teknologian käyttöaikomuksen määrääviin tekijöihin. Kysymyksien asettelu ja pieni viilaaminen oli aluksi melko haastavaa, mutta kun kysymykset aseteltiin siten, että haastateltavien oma kokemus tulee selkeästi ulos, muotoilu onnistui hyvin. Ensimmäinen haastattelu oli tärkeä olla koehaastatteluna, sillä kysymykset muuttuivat osittain seuraaviin haastatteluihin. Koehaastattelun tulokset tulevat mukaan tutkimukseen, sillä haastateltavan kokemukset olivat tutkimuksen kannalta sopivia. Puolistrukturoitu haastattelu toimi myös hyvin, sillä haastateltavien välillä oli eroja, joten haastatteluissa piti kysyä tarkentavia kysymyksiä ja alkuperäisten kysymyksien muotoilua joutui hieman muuttamaan haastatteluiden aikana.

Haastattelujen toteutus tapahtui etäyhteyden avulla. Kaikki haastattelut toteutettiin Zoom-palvelun kautta, koska se on vakiintunut työkalu Jyväskylän yliopistossa ja lisenssit ovat jaettu myös oppilaille. Olen kokenut sen helppokäyttöiseksi ja toimivaksi myös haastatteluita tehdessä. Haastatteluiden tallentamisen helppous oli yksi avaintekijöistä haastattelun toteuttamiseksi Zoomissa. Halusin varmistua haastatteluiden tallentamisella, ettei haastattelu mene hukkaan. Haastateltavilta ei kysytty henkilökohtaisia tietoja, joten haastateltavien anonymiteetti säilyi haastatteluiden läpi.

Luotettavuuden kannalta haastatteluissa painotettiin käyttäjän kokemusta. Kysymykset olivat neutraaleja, eikä niissä ollut johdattelua mukana. Jos haastateltavalta ei tullut johonkin kysymykseen vastausta tai hän ei ymmärtänyt kysymyksen tarkoitusta, annettiin haastateltavalle tarkentavia kysymyksiä.

Koehaastattelun jälkeen yksi kuva poistettiin (LIITE 3). Kuva oli haastattelussa käytetyn kuvan (LIITE 2) kaltainen, mutta siinä oli suppeampi valikoima maksuvaihtoehtoja ja kuvan tarkoituksena oli saada selville, minkä maksuvälineen haastateltava valitsisi suppeasta valikoimasta. Kuva poistettiin, koska siitä ei saanut mitään tärkeää tietoa.

Taulukossa 2 on esitelty haastateltavien tietoja sekä haastattelujen kestot. Haastateltavia oli yhteensä kahdeksan kappaletta, joista kuusi oli miehiä ja kaksi naisia. Tutkimus on varsin pieni, joten haastateltavien määrä on pyritty pitämään kohtuullisena. Kahdeksannen haastattelun jälkeen aineistoa koettiin saaneen tarpeeksi kattavasti tutkimuksen toteuttamiseksi, joten kahdeksan haastattelua oli riittävä. Ikäjakauma oli 23—27 vuotta ja keski-ikä 25 vuotta. Keskimäärin haastateltavat ovat tehneet verkko-ostoja viimeisen viikon aikana yhden kerran ja viimeisen kuukauden aikana 5,5 kertaa. Haastatteluiden keskipituus oli 19 minuuttia ja 52 sekuntia. Haastatteluiden pituus vaihteli haastateltavan persoonasta. Kaikille esitettiin samat kysymykset, lukuun ottamatta ensimmäistä koehaastateltavaa, mutta hänen haastattelunsa kesto ei johtunut siitä, vaan hänen pitkistä vastauksistaan.

TAULUKKO 2 Haastateltavien tiedot ja haastatteluiden kestot

	H1	H2	H3	H4	H5	H6	H7	H8	Keskiarvo
Ikä	25	25	26	23	27	25	24	25	25
Sukupuoli	mies	mies	mies	nainen	mies	mies	nainen	mies	
Ostoja viimeisen viikon aikana	0	2	0	0	0	5	0	1	1
Ostoja viimeisen kuukauden aikana	3	5	3	4	5	20	1	3	5,5
Haastattelun kesto	33:52	14:32	20:23	13:42	23:29	17:57	16:50	18:50	19:52

6 TULOKSET

Tässä kappaleessa käydään läpi empiirisen tutkimuksen tuloksia. Analyysissä keskityttiin kokemusten eroavaisuuksiin ja aiheen käsitysten eroavaisuuksien tutkimiseen. Haastattelujen aineisto on jaettu yhdeksään eri pääteemaan ja osalla niistä on alateemoja 1–3 kappaletta. Teemat ovat pääsääntöisesti samoja, kun haastattelun rungossa käytetyt teemat. Ensimmäinen ja toinen alaluku ovat analyysimenetelmän ensimmäistä tasoa, jossa pyritään tulkitsemaan haastateltavien tietämystä vahvasta tunnistautumisesta ja maksukäyttäytymisestä. Kolmannesta alaluvusta alkaen alaluvut ovat analyysimenetelmän toista tasoa, jossa haetaan käyttäjien kokemusta vahvasta tunnistautumisesta hyvinkin syvällisesti.

Ensimmäinen alaluku 6.1 käsittelee haastateltavien maksukäyttäytymistä ja maksuvälineiden suosioita, ja ne toimivat pohjatietoina seuraaville teemoille. Loput teemat ovat tutkimuksessa käytettyihin malleihin pohjautuvia. Alaluvussa 6.2 käydään läpi, miten tuttu vahva tunnistautuminen on haastateltaville. Alaluvussa 6.3 käydään läpi koettua helppokäyttöisyyttä ja vaivannäön odotuksia, sekä vahvasta tunnistautumisesta koettua nautintoa. Alaluvussa 6.4 käydään läpi koettua hyödyllisyyttä ja suorituskyvyn odotusta. Alaluvussa 6.5 käydään läpi tottumusta ja ala luvussa 6.6 asennetta. Alaluku 6.7käsittelee sosiaalista vaikutusta, 6.8 helpottavia olosuhteita ja viimeisessä alaluvussa 6.9 käsitellään uskottavuutta.

6.1 Maksuvälineet

Tämän teeman ensimmäinen alaluku sisältää maksuvälineiden suosiot ja syyt, miksi haastateltavan mielestä kyseinen maksuväline on mieluisin. Toinen käsittelee pankkikortilla maksamisen kokemuksia ja tunteita. Kolmas alaluku käsittelee haastateltavien maksukäyttäytymisen muutoksia, kuten eri välineiden haltuunottoa tai poisjättämistä. Neljäs alaluku käsittelee maksuvälineiden turvallisuutta, miten osa haastateltavista kokivat maksuvälineet turvallisuuden kannalta.

6.1.1 Mieluisin maksuväline

Haastateltavien keskuudessa mieluisimmat maksuvälineet olivat verkkopankki ja MobilePay. Osa haastateltavaa sanoi verkkopankin olevan mieluisin maksuväline ja osa sanoi MobilePayn olevan mieluisin maksuväline. Näiden lisäksi yksi sanoi aluksi MobilePayn

olevan mieluisin maksuväline, mutta huomattuaan PayPalin, hän vaihtoikin mieluisimmaksi PayPalin. Hän kuitenkin sanoi, että pienissä ostoksissa hän käyttää MobilePayta hyvin paljon.

> ”No mobilepay, jos se vaan on. […] No sittenkin ehkä, jos ostaa jotain vähän kalliimpaa niin PayPal on mieluisin, koska sieltä saa rahat helpoiten takaisin sen kautta. Mutta jos ostaa jotain pientä, niin maksaa MobilePaylla, koska se on helpoin kaikista.” (H6)

Verkkopankkimaksua perusteltiin mieluisimmaksi tottumuksen, helppouden ja turvallisuuden perusteella. Näkemykset hajaantuivat hieman, mutta tottumus oli perusteena kolmella neljästä haastateltavista ja helppous kahdella. Yksi haastateltavista perusteli verkkopankkimaksua myös turvalliseksi, ja lisäksi toinen sanoi kaikkien maksuvälineiden olevan turvallisia. Bezovskin (2016) mukaan turvallisuus on ihmisten tärkein huolenaihe kaiken teknologian käytössä. Haastateltavien kokemuksen perusteella käyttäjät pääsääntöisesti pitävät maksuvälineitä, etenkin verkkopankkimaksamista, turvallisina.

> ”Kyllä se on turvallisuus ja tottumus, koska niinku just se niinku… se on varmasti enemmän tottumus ku turvallisuus, mutta ehkä just kun sitä on tottunut käyttämään niin sitä kautta se turvallisuuskin tulee, et aikaisemmin nimenomaan, ku oli pelkästään se tunnuslukukortti, niin sen koki tosi turvallisesks, ku tiesi, että tää on vaan mulla tää ja vaan mä voin päästä mun pankkiin sillon ku mä haluan. Toki, kyl se niinku et käytetäänhän tossa biometristä tunnistusta tossa sovelluksessa, mikä on tavallaan sama asia mut kyl turvallisuus ja tottumus on tos ne, ku mulla on danskebank ollu koko ikäni ni se varmasti myös vaikuttaa jo pelkästään, ku näkee sen logon, ni se tuo semmosen että tätä kautta homma hoituu turvallisesti” (H1)

> ”Joo ainaki tottumus tietysti. Lähtökohtasesti tuntuu, että nää on kaikki turvallisia. Koen, että on ihan yhtä turvallinen, maksatko sä pankin kautta vai pankkikortilla.” (H3)

Yksi haastateltava, joka perusteli verkkopankin maksamista muun muassa turvallisena, käytti tietokoneellaan virustorjuntaa. Virustorjunta laittaa tietokoneeseen erityissuojaukset päälle aina, kun käyttäjä vierailee selaimellaan verkkopankissa.

> ”Joo kyllä ja siinä on just se, että tietokoneella maksamiseen linkittyy se, että mulla on virustorjunta koneella, joka ku mä kirjaudun pankkiin ni se tunnistaa, että mä oon pankissa, jolloin se laittaa semmoset erityissuojaukset päälle ja se tulee näkymään ihan tähän näytölle, että tulee semmoset reunukset tohon näytön reunaan ja sitten tietää, että voi turvallisesti käyttää pankkia.” (H1)

Haastateltavat, jotka sanoivat MobilePayn olevan mieluisin maksuväline, perustelivat sitä yksimielisesti MobilePayn olevan helppo ja nopea maksuväline ja siksi ne käyttävät sitä aina, kun se on tarjolla. Osa heistä mainitsi myös, että jos MobilePay on tarjolla, he sen valitsevat. Tästä päätellen verkkokaupat eivät läheskään aina sitä vaihtoehtoa vieläkään tarjoa. MobilePay on tullut viimeisen kahden vuoden aikana yhä useamman verkkokaupan valikoimiin, mutta se ei ole selvästikään vielä vakuuttanut kaikkia kauppiaita, koska sitä ei niin monessa verkkokaupassa ole tarjolla, että se täytyy erikseen mainita, että jos löytyy.

> ” […] jos on tarjolla se MobilePay, niin sen valitsen mielummin kuin, että alkais näpyttelemään kortin tietoja ja vielä lisäksi tunnistautuu.” (H3)

> ” […] Jos ei ois MobilePayta tossa niin varmaan ottaisin ton Osuuspankki tai ton pankkijutun, mutta siinä on enemmän niitä tietoja, mitä pitää syöttää sinne. Tuntuu, että toi MobilePay ois helpoin näistä.” (H7)

Kaikki haastateltavat kokivat, että verkkokaupan maksuvaihtoehtoja on riittävästi tai heillä ei ole tullut vastaan sellaista tilannetta, että olisi ollut liian vähän vaihtoehtoja tarjolla.

> ”Joo, mä en muista ainakaan, että oisin ajatellut, että verkkokaupoilla ei olisi tarjolla itselle sopivaa tapaa, että kyllä se löytyy useimmiten.” (H8)

6.1.2 Pankkikortilla maksamisen kokemus

Kaikki haastateltavat olivat vähintään joskus testannut pankkikortilla maksamista. Se olikin yksi haastateltavien hyväksymisen ehto. Kokemuksena pankkikorttimaksu koettiin turhauttavana ja turhana, koska siinä tarvitaan vahvan tunnistautumisen myötä ylimääräinen työvaihe eli verkkopankissa tunnistautuminen. Osa sanoi, ettei maksa pankkikortilla tai ei edes laita pankkikortin tietoja mihinkään, ellei ole aivan pakko tilatakseen jonkin tuotteen tai palvelun.

> ”Yleensä en kortin tietoja kovin mielellään laita mihinkään. Joskus on tarvinnu ku ei oo muita vaihtoehtoja ollu saatavilla.” (H2)

> ”No se on vähän vaivalloista. Se vähän riippuu, jos se vaatii sen tunnistautumisen sieltä pankin kautta, niin se on vaivalloista, mutta jos se on ainut vaihtoehto ni sitten se on pakko maksaa sillä. ” (H4)

> ” […] En tiiä, onko sitten ollut pakko tehdä, että ei oo muuta voinut valita.” (H5)

Edellisten lisäksi yksi haastateltavista käyttää myös pankkikorttia vain pakon edessä. Hän kuitenkin käyttää luottokorttia kalliimpien tavaroiden tilaamiseen, koska jos tuotteen palauttaa, niin ei tarvitse turhaan maksaa ja palauttaa rahoja.

> ”Se on vähän semmonen, ku siinä pitää tehä se vahvistaminen siellä verkkopankin kautta. Ni se on vähän hidas ja se ärsyttää. Mutta se on sillai hyvä, että muuten vois melkeen kuka vaan ostaa sillä sun kortilla. Että sen takia en käytä sitä niin paljon, jos ei oo pakko, ku siinä on se vahva tunnistautuminen. On siinä se hyvä, että jos haluaa ostaa jonkun kalliimman tuotteen netistä, ja jos ei tiiä, onko se sopiva tai onko se hyvä, ni sen voi ostaa luoton kautta sen tuotteen ja sen voi palauttaa sen tuotteen, ni ei turhaan maksa.” (H3)

Pankkikortilla maksaminen koettiin hyvin eri tavalla haastateltavien välillä. Osa haastateltavista koki pankkikortilla maksamisen turhauttavalta, kun taas osa koki pankkikortilla maksamisen helpoksi tavaksi. Yksi haastateltava perusteli pankkikortilla maksamisen helppoutta sillä, että hän oli tallentanut kortin tiedot puhelimeensa.

> ”No se on aika helppoa, koska mulla tulee puhelimessa ne kortin tiedot automaattisesti siihen, mutta silti musta tuntuu, että ottaisin ton MobilePayn aina, jos se on siinä vaihtoehtona.” (H7)

6.1.3 Maksukäyttäytymisen muutos

Maksukäyttäytymisen muutoksesta kysyttäessä, osa vastasi kokeneensa muutoksia maksukäyttäytymisessä. Ensimmäiseltä koehaastateltavalta tätä ei kysytty. Muutokset ovat olleet joko pankkikorttimaksun vähentämistä tai MobilePaylla maksamisen lisäämistä. Joidenkin haastateltavien maksukäyttäytyminen koetaan muuttuvan fyysisistä korteista puhelimella maksamiseen eli mobiilimaksamiseen.

> ”Joo kyllä. Kyllä mä sillon käytin pankkikorttimaksua enemmän, kun ei ollut vahvaa tunnistautumista. Ne tiedot oli nopea laittaa ja se oli sillä selvä, että kyllä se vahva tunnistautuminen on ollut isoin syy sen tavan vähentämiseen.” (H3)

> ”Joo kyllä mä suosin nykyään puhelinta mahdollisimman paljon, että en fyysisiä kortteja. Just MobilePayta, joka menee kasvojentunnistuksen kautta ni ei tarvi käyttää mitään koodeja. Kyllä se menee koko ajan helpompaan ja nopeampaan suuntaan.” (H8)

6.2 Vahvan tunnistautumisen tuntemus

Vahva tunnistautuminen yleisellä tasolla oli kaikille tuttu asia ja kaikki tiesivät mistä on kysymys. Näkyvimpänä vahva tunnistautuminen oli näkynyt haastateltaville pankkikortilla maksaessa, kun täytyy tunnistautua pankkitunnuksilla. Osa heistä mainitsi, että viimeisen vuoden aikana tunnistautuminen on lisääntynyt. Pankkikorttimaksuihin onkin tullut vahva tunnistautuminen pakolliseksi tammikuussa 2021 (Finanssivalvonta, 2019b).

> ”Oon kuullu, ja jos tarkotat sitä, että kun pankkikortilla maksaa niin se kysyy vielä lisäksi nettipankkitunnuksia.” (H2)

> ”Joo oon kyllä huomannu. Sitä on ainakin vuoden ajan, jopa vähän enemmänkin kysytty kyllä.” (H3)

> ”Joo ja oon huomannu, että se pitää nykyään useammin käydä se mobiiliavain syöttämässä.” (H7)

Yksi haastateltavista puolestaan sanoi, että hän on kuullut vahvan tunnistautumisen tulevan, mutta hän on sivuuttanut tai jopa unohtanut jo asian, koska hän maksaa nykyään niin harvoin pankkikortilla verkkomaksujaan.

> ”Mä en kyllä nyt muista, että kysytäänkö sitä siinäkin. Sittenhän se on vielä monimutkaisempaa kortin tiedoilla maksaminen, mutta joo mä tiän kyllä ton, että se on tullu. Mä varmaan oon sen sivuuttanut. Tosi harvoin mä kortilla oon nykyään maksanut.” (H5)

6.3 Koettu helppokäyttöisyys ja vaivannäön odotukset

Haastateltavat olivat melko yhtä mieltä koetusta helppokäyttöisyydestä ja vaivannäön odotuksista. Vahva tunnistautuminen on pankkikortilla maksaessa koettu helppokäyttöiseksi, mutta turhaksi. Vaivannäön odotukset UTAUT-malleissa tarkoittavat koettua helppokäyttöisyyttä ja sitä, kuinka helposti teknologiaa oppii käyttämään (Venkatesh, 2003). Vahva tunnistautuminen ei ole etukäteen ajateltuna kovin vaikeakäyttöistä teknologiaa, eikä se haastatteluiden perusteella sitä myöskään ollut.

> ”No on se ollut helppokäyttöinen, että ei se vahvistamisprosessi oo vaikea, että sä vaan näppäilet ne sun koodit vaan. Mutta se, että joutuu sen maksamisen lisäksi näpytellä sitä ylimäärästä, niin se on mikä on saattanut hiertää, kun menee aikaa. Mutta ei nyt ikinä niin kiire oo ettei minuuttia tai oikeestaan kymmentä sekunttia kerkeis siihen käyttää.” (H3)

> ”Kyllä se on helppokäyttöinen, mutta mua turhauttaa se, että jos sä oot jossakin ja sun pitää lähteä tunnistautumaan sinne, niin sun pitää hyppiä niiden sovellusten välillä, jos vaikka teet puhelimella. Mutta ei siinä oo mitään ongelmaa, että kun käy vaan syöttämässä sen yhden koodin sinne toiseen sovellukseen, mutta onhan se aina enemmän säätöä. ” (H7)

Vahvan tunnistautumisen kokemus muissa maksutavoissa on koettu huomaamattomaksi ja siihen suuntaan ollaan menossa, että maksamisen pitää olla helppoa ja nopeaa eli siinä ei saa olla ylimääräisiltä tuntuvia vaiheita (Zhong ym., 2021). Vahva tunnistautuminen on hidastanut pankkikortilla maksamista ja näin ollen nopeammat maksutavat tulevat suosituimmiksi.

> ” […] Siks mä oon siirtynyt niihin maksutapoihin, että niissä mä koen, että niitä on nopeempi käyttää, niissä on vähemmän näpyteltävää ja se tekee itselle ostamisen helpommaksi. Sitten se on luontevampi mennä sen mukaan, mikä on nopeampi ja helpompi.” (H8)

> ”Siinä se on huomaamatta tullut. Se on se miten ne nykyisin toimii. Joskus se muuttuu ja sitten se on semmonen.” (H5)

MobilePay koettiin hieman yllättäen muihin vastauksiin nähden lähes vastaavana kuin pankkikortilla maksamisen. Molemmissa maksutavoissa pitää mennä puhelimen sovellukseen vahvistamaan tapahtuma. Vaikka ne hyvin samanlaisilta tuntuvat, mobiilimaksaminen koettiin silti helpommalta ja mutkattomammalta, koska siinä ei tarvitse syöttää muita lukuja kuin MobilePayn pinkoodin. Pankkikorttimaksaminen onkin huomattavasti helpompaa silloin, kun käyttää tallennettuja kortin tietoja ja automaattista täyttämistä, mutta ilman niitä pankkikorttimaksaminen on vaivalloista.

> ”Öö, no tavallaan kyllähän sä joudut MobilePayhinkin menemään ja syöttämään sen koodin. Mutta tuntuu, että se on vähän niinku, jos vaikka ajattelee, että tuosta valitsis tuon MobilePayn, niin se menee suoraan siihen MobilePayhin, eikä sun tarvi alkaa korttitietoja syöttämään. Niin se tuntuu periaatteessa helpommalta ja mutkattomammalta. Jos ei esimerkiks ois kortin tietoja tallennettuna, niin pitäis alkaa ettimään se kortti tai miettimään, mitkä ne oli ne luvut.” (H7)

Yksi haastateltava koki ongelmia vahvassa tunnistautumisessa. Toki hän koki sen itselleen helppokäyttöisenä, mutta teknologian kanssa on ollut myös ongelmia. Hän sanoi, että käyttäjän tunnistautumisvaiheessa järjestelmä on kaatunut välillä ja tapahtuma on pitänyt aloittaa alusta. Hän on tällaisissa tapauksissa aina käynyt tarkistamassa pankkitililtä,

ettei tapahtumaa ole veloitettu kahteen kertaan. Täyttä luottoa teknologiaan ei ole pystynyt antaa.

> ”No kyllä se on keskimäärin aika helppokäyttöinen eli välillä on tullu semmosia niinku bugeja esimerkiksi on jostain syystä se ei oo tullu se pyyntö siihen sovellukseen, että pystyis hyväksymään sen ja jostain syystä on vaikka tullu aikakatkaisu verkkokaupassa, että sitten on joutunu alottaa koko homman niinku uudestaa, että on joutunu sen hyväksymisen tehdä toiseen kertaan. Aika harvoin noita on tullu ja noissa tapauksissa on käyny vielä tupla tarkistamassa oman pankkitilin ettei oo lähteny maksu kahteen kertaan tai jotain tämmöstä, mut aika hyvin se sillein on toiminu et en oo kokenu sitä ku puhelin kuitenkin jos koneella oon ni puhelin on tossa lähellä ni se on helppo sitä kautta.” (H1)

6.4 Koettu hyödyllisyys ja suorituskyvyn odotukset

Useimmat haastateltavista kokivat, että he eivät ole saaneet vahvasta tunnistautumisesta henkilökohtaisella tasolla itselleen mitään hyötyä. Lähes kaikki heistä sanoivat kuitenkin ymmärtävänsä sen, että sillä haetaan turvallisuutta verkkomaksamiseen. Yksi sanoi vahvasta tunnistautumisesta olevan hyötyä henkilökohtaisella tasolla siten, että maksettaessa pankkikortilla pitää mennä hyväksymään maksu pankista, niin pankki ilmoittaa mihin rahat ovat menossa. Tämä luo kuluttajalle turvallisuuden tuntua, kun varmistuu siitä, että rahat menevät oikeaan osoitteeseen.

> ” […] mun täytyy nimenomaan mun sormenjäljellä niinku tavallaan se tunnuslukusovellus avata, käydä sieltä hyväksymässä ja siinä lukee se, että mihin rahat on liikahtamassa. Kyl se itselle siinä on ehkä tuonu semmosta hyötyä, semmosta turvaa siinä, että tietää mihin, et just mä oon ite nimenomaan ostamassa tän jutun ja mä hyväksyn tän maksun. Siinä on tavallan se et mä oon digannu siinä mielessä tunnuslukusovelluksen käytöstä.” (H1)

Kun vahva tunnistautuminen tuli osaksi pankkikorttimaksamista, se herätti ihmetystä haastateltavissa. Jotkut heistä kyseenalaistivat uuden teknologian ja miettivät, että miksi ja mihin tarkoitukseen tällaista teknologiaa tarvitsee.

> ”No vähän mä ihmettelin, että miks sillon tarvi tunnistautua, kun aikasemmin ei oo tarvinnut. Mutta ihan järkeväähän se on tietoturvan kannalta.” (H2)

> ”Aluksi oli sillein, että mitä ihmettä? Miksi näitä kysellään tässä vähän niin kuin ns uudestaan […] ” (H4)

6.5 Tottumus

Vahvaan tunnistautumiseen haastateltavat ovat kokeneet tottuneen melko hyvin ja nykyään se on automaattinen toimenpide, mikä kuuluu verkkokaupan maksuprosessiin maksettaessa pankkikortilla.

> ”Ei kai siitä mitään ihmeempiä. Kyllähän siihen aika nopeesti tottui. Ei se ollu mikään isompi kriisi.” (H3)

Puolestaan eräs haastateltavista oli tottunut välttelemään pankkikorttimaksussa vaadittavaa vahvaa tunnistautumista viimeiseen asti, koska hän on kokenut pankkikortilla maksamisen tulleen turhaksi maksuvälineeksi.

> ”No oon mä tottunu, mutta lähtökohtaisesti oon tottunut välttelemään sitä, että en käytä sitä vähän niinku ylimäärästä tunnistautumista, jos se ei oo välttämätön.” (H6)

6.5.1 Vahvan tunnistautumisen vaikutus maksukäyttäytymiseen

Kuten kappaleessa 6.1.3 kerrotaan, haastateltavat ovat muuttaneet viime vuosien aikana maksukäyttäytymistään. Osa haastateltavista ei ole kokenut pankkikortilla maksamiseen tullutta vahvaa tunnistautumista omakseen. Puolestaan he ovat muuttaneet maksukäyttäytymistä vahvan tunnistautumisen takia. He kokivat muun muassa, että aikaisemmin kortilla maksaminen oli helppoa ja nopeaa kun syötti vain kortin tiedot. Kun nyt sen lisäksi pitää vielä tunnistautua pankkitunnuksilla, he jättivät maksutavan kokonaan pois, tai maksavat sillä vain, jos on aivan pakko. Tilalle he ovat etsineet helpompia maksutapoja, kuten MobilePayn.

> ”Joo kyllä. Kyllä mä sillon käytin pankkikorttimaksua enemmän kun ei ollut vahvaa tunnistautumista. Ne tiedot oli nopea laittaa ja se oli sillä selvä, että kyllä se vahva tunnistautuminen on ollut isoin syy sen tavan vähentämiseen.” (H3)

> ”Ei oikeestaa, tai no sen, että jos on tarjolla se MobilePay, niin sen valitsen mielummin kuin, että alkais näpyttelemään kortin tietoja ja vielä lisäksi tunnistautuu. ” (H4)

> ”Käytin paljon enemmän. **Ja tämän takia oot jättänyt sen pois?** H6: Kyllä. ” (H6)

> ”Joo oon siirtynyt muun muassa MobilePayhyn. Oon etsinyt helpompia tapoja maksaa. ” (H8)

Eräs haastateltavista on kokenut pankkikortilla maksamisen jopa niin turhauttavaksi, että hän perui maksutapahtuman ja aloitti maksutapahtuman alusta toisella maksuvälineellä, jos hän oli valinnut pankkikortilla maksamisen maksuvälineeksi ja huomannut sen vaativan vahvaa tunnistautumista.

> H3: Joo kyllä se on vaikuttanu siihen, että alkuun sitä ei oikeen muistanut, kun pankkikortilla maksoi, ni siinä kun tuli se vahvistautuminen niin sitä saattoi tyyliin perua sen maksutapahtuman ja saatto sitten mennä omilla pankkitunnuksilla uudestaan maksamaan ku ärsytti niin paljon. Kyllä se on siihen vaikuttanut, että en mä pankkikorttimaksua enää käytä, jos ei oo pakko. Se on nopeempi oman pankin kautta suoraan.

6.6 Asenne

Asenteessa vahvaa tunnistautumista kohtaan on havaittavissa jonkinlaista hajaannusta. Haastateltavista kolmella on hyvä asenne vahvaa tunnistautumista kohtaa, kolmella neutraali ja yhdellä kielteinen. Positiivisesti vahvaa tunnistautumista kohtaa suhtautuvat tykkäävät, että tietoturva on kunnossa. Osa heistä kokivat silti turhautumista vahvaa tunnistautumista kohtaan, mutta heille on silti tärkeämpää turvallisuus kuin pieni turhautuminen.

> ”No ite tykkään, että tietoturva on kunnossa, niin se on positiivinen asia.” (H2)

> ”Suhtaudun siihen ihan hyvin, mutta välillä jos on hirvee kiire maksaa ni sitten ärsyttää kun joutuu ylimääräsiä näpytellä. Mutta kyllä se on kumminkin hyvä, että se tunnistautuminen on.” (H3)

> ”Niinku mä aluksikin sanoin, niin välillä vähän turhauttaa. Mutta kyllä mä koen, että se on sellanen luotettava juttu. Että semmonen hyvä asenne.” (H7)

Neutraalisti vahvaa tunnistautumista kohtaan suhtautuvia ei vahva tunnistautuminen ärsytä, mutta he eivät myöskään koe siitä olevan erityisesti mitään hyötyäkään. He ovat jo kokeneet tottuneen siihen, joten asenne on hyvin neutraali.

> ”Sillai aika neutraali, että ei se mua mitenkään sillai ärsytä, mutta se on vähän niinku semmonen pakollinen paha, mikä pitää aina sitten tehdä.” (H4)

> ”Se on se miten toi homma toimii. Ei mitään sitä vastaan ja varmasti siinä jotain hyvää on. Ei se oo mitenkään monimutkaistanu mitään.” (H5)

> ”No hyvin neutraali. Ei herätä vihaa tai kauhistusta ja ymmärrän, miks sitä pyydetään, mutta on se vähän, kun ehti tottua siihen, kun sitä ei jossain välissä kysytty niin paljon.” (H8)

Yksi haastateltavista kuitenkin kertoi suhtautuvansa kielteisesti ja välttelevästi vahvaa tunnistautumista kohtaan. Pankkikorttimaksamisesta on tullut siihen kuuluvan vahvan tunnistautumisen jälkeen turha maksuväline, joka on sama kuin verkkopankkimaksu, mutta siinä on vain lisäksi yksi vaihe, jossa pitää syöttää oman pankkikortin tiedot internettiin.

> ”Vähän ehkä semmonen kielteinen asenne, koska kyllä mä ymmärrän sen tarpeellisuuden periaatteessa, mutta sitte taas ku se vaikeuttaa sitä niin paljon, että muista vaihtoehdoista, kuten suoraan verkkopankilla maksamisesta, tulee niin paljon helpompaa, koska siinä poistuu vaan yksi vaihe niin mä teen periaatteessa sen saman tunnistautumisen ilman pankkikorttia, koska kortilla maksaessa siinä on vain yksi ylimääräinen vaihe. Periaatteessa semmonen kielteinen tai välttelevä asenne korttimaksua kohtaan.” (H6)

6.7 Sosiaalinen vaikutus

Sosiaalisesta vaikutuksesta haastateltavilta kysyttiin niin vahvasta tunnistautumisesta kuin maksutavan valinnasta, sillä koin tarpeelliseksi tietää myös maksutavan valinnan sosiaalisen vaikutuksen toista tutkimuskysymystä ajatellen.

6.7.1 Sosiaalinen vaikutus vahvaan tunnistautumiseen

Sosiaalinen vaikutus vahvassa tunnistautumisessa oli hyvin yksimielistä. Kukaan haastateltavista ei kokenut, että heidän suhtautumiseensa olisi vaikuttanut läheisten mielipiteet tai kokemukset, koska asiasta ei ole heidän kanssaan puhuttu lainkaan. Tämä on varmasti harvinaisempi puheenaihe ja kokemukset siitä ovat tulleet omasta käytöstä ja sitä kautta myös suhtautuminen vahvaan tunnistautumiseen on henkilökohtainen mielipide kokemukseen perustuen.

6.7.2 Sosiaalinen vaikutus maksuvälineen valinnassa

Puolestaan maksutavan valinnassa sosiaalisella vaikutuksella oli osuutta. Puolet haastateltavista oli kokenut, että kaverit ovat olleet vaikuttamassa maksutavan valintaan. Osa on ottanut esimerkiksi MobilePayn tai MobilePayn päälle rakennetun WeSharen käyttöön kavereiden vaikutuksesta. Eräs haastateltavista kertoi, että perheen (vanhempien) kautta hän on avannut pankkitilin ja täten myös verkkopankkimaksu on tullut perheen vaikutuksesta. Tämä onkin hyvin luonnollinen tapa ottaa verkkopankkimaksu käyttöön yhtenä maksuvälineenä.

> ”Mut nyt ku sanoit tosta et ehkä siinä tavallaan huomaa kun sillon vaikka kun mobilpay tuli niin sitä ei aluksi tai en ehkä ihan heti ollu tai otin aika nopeesti haltuun, mutta siinä huomas sen kavereitten merkityksen, että sehän sitäkin kautta sitä ruvettiin käyttää enemmän, koska sillä ruvettiin jakamaan reissujen kuluja ja tämmöstä. Et siinä huomas sen sosiaalisen vaikutuksen. Että ite käytin mobilepayta, mut sitte aloin käyttää wesharea ku kaverit sano, että laitetaan sinne kaikki kulut. Se linkittyy myös tohon mobilepayhyn.” (H1)

> ”Varmasti MobilePay on tullut sitä kautta, että kaverin kanssa on käyttänyt ja sitten on saattanut verkko-ostoksiakin sillä tehdä. Ja no tottakai perhe on vaikuttanut lähtökohtaisesti aiempaan ja nykyiseenkin pankkiiin mitä käytän myös verkkomaksuissa. ” (H5)

Eräs haastateltavista on testannut PayPalia kaverin suosituksesta ja sitten hyväksi todettuaan ottanut sen myös käyttöönsä.

> ”Joo PayPalia oon käyttäny sen takia, kun yks kaveri suositteli sitä. Ja oon sen jälkeen käyttänyt sitä paljonkin. ” (H6)

Yksi haastateltavista kokee yleisellä tasolla uusien maksuvälineiden vaikuttaneen hänen maksukäyttäytymiseensä. Hän ei mainitse mitään maksuvälinettä nimeltä, mutta hän on keskustellut kavereiden kanssa uusista maksuvälineistä. Haastateltava kokee päättävänsä silti itse, ottaako hän käyttöön uuden maksuvälineen tai testaako hän kyseistä maksuvälinettä.

> ”Varmaan kavereiden kanssa jutellaan, jos tulee uutta maksutapaa. Sitten varmaan ottaa helpommin käyttöön jonkun uuden maksutavan, jos joku muu on koittanut. Käytännössä ite tekee ne päätökset. ” (H3)

6.8 Helpottavat olosuhteet

Helpottaviin olosuhteisiin kuuluvat teknologiaosaaminen sekä muu teknologia, joka helpottaa vahvan tunnistautumisen omaksumista. Helpottavia olosuhteita joko vaaditaan teknologian käytössä tai sitten ne tukevat sen käyttöä. (Venkatesh, 2003).

6.8.1 Teknologiaosaaminen

Teknologiaosaamisen vaikutus helpottavana taitona vahvan tunnistautumisen omaksumisessa on koettu kolmella eri tavalla: Ensinnäkin osa haastateltavista sanoi sen helpottavan ymmärtämään, miksi vahva tunnistautuminen on pakollinen ja sitä kautta se vaikuttaa positiivisesti myös suhtautumiseen vahvaa tunnistautumista kohtaan.

> ”Mmm, mä sanoisin tohon ehkä, että silleen että mä ymmärrän sen, että mitä siinä tapahtuu, miksi se kannattaa tai miksi se pitää tehä noin.” (H1)

> ”No ehkä se vaikuttaa, että jos vähä ymmärtää niin siihen suhtautuu eri tavalla, ettei sitä ajattele semmosena turhana asiana. Että tajuaa sen, miksi se on tehty.” (H2)

Toiseksi haastateltavat sanoivat, että teknologiaosaamisesta on ollut sen verran hyötyä, että vahvan tunnistautumisen käyttöönotossa ei ole ollut teknisiä ongelmia ja sen käyttäminen oli vaivatonta heti alusta alkaen. Vahva tunnistautuminen on tullut kuin itsestään käyttöön.

> ”No ei siinä oo ainakaan mitään ongelmaa ollut itellä käyttää sitä. Vähän vaikea kuvitella, että jollakin olis, mutta varmasti jollakin on siinä ongelmaa. Aika simppeli se on sillai.” (H5)

> ”Joo on, ja sitä ei oo tarvinnut opetella vaan se on ihan perusjuttu. Tavallaan siksi se tunnistautuminen on ihan huomaamatta tullut. Sitä ei oo ajatellut että se on nyt vuosi sitten tullut ja viimesen vuoden aikana lisääntynyt ku se on semmonen perusjuttu.” (H7)

Kolmanneksi haastateltavat kokivat, että teknologiataidot ovat auttaneet tajuamaan nopeasti, miten vahvaa tunnistautumista on nopea käyttää ja miten sitä on turvallista käyttää. Nopeuteen vaikuttavia tekijöitä ovat esimerkiksi automaattinen tunnusten täyttäminen tai ulkoa opettelu. Turvallisinta on ulkoa opettelu ja vähemmän turvallista on automaattinen tunnusten täyttäminen, vaikkakin sekin on hyvin turvallinen, kun yleensä tietojen täyttäminen vaatii biometrisen tunnistautumisen.

> ”Kyllä se varmasti vaikuttaa sillä tavalla, että se ei oo mikään ongelma se vahvan tunnistautumisen prosessi, että nopeesti tajuaa sitten, miten sen pystyy nopeiten tehä ja mikä on turvallinen tapa tehdä se.” (H3)

> ”No mä koen, että.. ehkä se tulee siitä ku mennään puhelimen puolelle, että mä oon osannu ehkä hyödyntää puhelimessa just kasvojentunnistusta ja mahollisimman paljon automaattisia salasanoja ja muita, että sitä kautta oon oppinu käyttämään teknologian noita ominaisuuksia.” (H8)

6.8.2 Muut helpottavat teknologiat

Muuta teknologiaa, jota haastateltavilla oli käytössään vahvan tunnistautumisen prosessissa, olivat biometrinen tunnistautuminen ja automaattinen tietojen täyttäminen, kuten edellisessä kappaleessa tuli esille. Monet heistä käyttävät biometristä tunnistautumista ja yksi käyttää sen lisäksi vielä automaattista tietojen täyttämistä, kuten verkkopankkitunnusten täyttämistä.

> ”Joo mulla on tallennettuna verkkopankkitunnukset puhelimessa, salasanojen takana tottakai, mutta ne tulee automaattisesti sieltä sillai, että ei tarvi muistaakseni mitään salasanaa syöttää, että se menee kasvojentunnistuksella läpi parhaimmillaan.” (H8)

6.9 Uskottavuus

Uskottavuus sisältää käyttäjän kokemia turvallisuus- ja yksityisyysuhkia uuden teknologian käytössä. Haastateltavista suurin osa koki vahvan tunnistautumisen olevan turvallisuutta edistävää teknologiaa ja vahvassa tunnistautumisessa ei ole mitään uhkia itsessään. Yksi mainitsi, että uhat ovat enemmän siellä verkkokaupan päässä ja osa haastateltavista mainitsi, että vahva tunnistautuminen vaikeuttaa kadonneen kortin väärinkäyttöä rikollisessa tarkoituksessa.

> ”No en mä usko, että tossa sinänsä on, että todennäköisesti ne uhat on enemmän siellä verkkokaupan päässä ja sitten tohon tulee vaan toi pankin palvelu mukaan.” (H5)

> ”No joo kyllä mä sen takia, että pankkikortin katoamiset ja tämmöset ei oo ehkä enää niin iso juttu, jos ei niillä voi niin helposti maksaa enää ilman sitä tunnistautumista, niin sinällään joo kyllä. En tiiä miten muuten mä siinä kokisin turvallisuutta edistävänä.” (H6)

> ”Kyllä. Sehän lisää taas yhen esteen siihen, jos joku haluaa päästä mun maksutietoihin tai muihin. Kyllä mä koen, että se lisää turvallisuutta.” (H8)

Vahvan tunnistautumisen uhista eräs haastateltavista sanoi esimerkin, että EU:n ulkopuolelta ostettaessa, vahvaa tunnistautumista ei kysytä. Toinen koki muun muassa tällaisten mahdollisen tapauksen vaikuttavan negatiivisesti vahvan tunnistautumisen uskottavuuteen kuvaamalla sitä puoliturhaksi.

> ”Se missä ite koen, että vahva tunnistautuminen ei vielä näy, on se, että jos mä ostan videopeleissä pelin sisäisiä ostoja. Eli tarkoitan esimerkiksi League of Legendsiä ja mä haluan siellä ostaa itelleni uusia skinejä, mä tarviin siihen oikeeta rahaa. Siellä se homma toimii siten, että mun tarvii syöttää ainoastaan kortin tiedot ja sitten painaa hyväksy. Toki siitä tulee kuitit sähköpostiin. Se on käsittääkseni jenkkiläinen se yritys, kenelle ne maksut menee.” (H1)

> ”Jep, se on niin että, jos se ei oo aina, niin se on puoliturha. Johonki ne saa aina maksettua.” (H6)

Yksi haastateltavista koki luottavansa vahvaa tunnistautumista tarjoaviin palveluntarjoajiin, mutta yksi toinen taas sanoi välttävänsä sellaisia tapahtumia, missä pitää tunnistautua palveluun. Hän kokee pelkoa menettää omia tietoja rikollisille. Tällaisia tilanteita voisi olla esimerkiksi väärennetyt sivut, jotka näyttävät oikeilta, mutta keräävätkin tietoja.

> ”No kyllä mä sen, että riippuen mihin on tunnistautumassa ja mistä on ostamassa, niin pyrin välttämään sitä, että yhtään mihinkään tunnistautuis tai kirjautuis niillä. No siinä on joku pieni pelko, että jos siinä ois joku, minkä kautta vois menettää jotain ja joku voi saada haltuun ne. Vaikka yleensä ne on jonkun tunnetun palveluntarjoajan kautta se tunnistautuminen, mutta joka tapauksessa.” (H6)

> ”En oo, että mä oon luottanu aika hyvin noihin palveluntarjoajiin. Että en oo sinänsä osannu pelätä semmosta uhkaa.” (H8)

Yksi haastateltavista puolestaan pohti sellaista tilannetta, missä rikollinen saa laitteen haltuun, missä on eri tunnuslukuja, mutta totesi itse siihen, että sen lisäksi pitäisi tietää vielä

4–5 koodia, jotta pystyy käyttämään tunnistautumistietoja, joten kyseessä ei ole varsinainen uhka.

> ”Tavallaan siinä on sitten se, että jos saa sen laitteen haltuun, on siinä toki sitten erilaisia tunnuslukuja mitä tarvii vielä sen lisäksi, mahdollisesti jopa neljä tai viisi, onko pin-koodia ja muuta.” (H5)

7 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tarkoituksena oli tutkia, miten vahvan tunnistautumisen käyttöönotto on koettu ja onko se koettu vaikuttaneen maksukäyttäytymiseen. Tutkimuksen empiirinen aineisto kerättiin yksilöhaastatteluna puolistrukturoidulla menetelmällä ja tutkimukseen osallistui kahdeksan haastateltavaa, joista ensimmäinen toimi koehaastateltavana. Aineiston analysoinnissa käytettiin fenomenografista analyysia. Tutkimuksen tutkimuskysymykset olivat

- Miten kuluttajat ovat kokeneet vahvan tunnistautumisen käyttöönoton?
- Miten vahvan tunnistautumisen on koettu vaikuttavan maksukäyttäytymiseen?

Tässä luvussa kerättyä aineistoa peilataan tietojärjestelmätieteen aiempaan tutkimukseen teknologian omaksumisesta. Johtopäätökset tutkimustuloksista esitellään luvussa 7.1 ja tutkimuksen luotettavuutta ja toistettavuutta sekä tutkimusta tehdessä ilmenneitä jatkotutkimusaiheita tarkastellaan luvussa 7.2.

7.1 Johtopäätökset

Tutkimuksen teoriaviitekehyksenä toimi tietojärjestelmätieteen teoria UTAUT2, joka on kuluttajan teknologian hyväksymistä kuvaava malli. Mallia muokattiin hieman spesifimmäksi juuri vahvaa tunnistautumista koskevaksi, sillä alkuperäinen malli ei olisi antanut niin paljon informaatiota, mitä olisi tarvinnut ja osa olisi ollut turhaa. Muokattu versio UTAUT2-mallista on esitelty kuviossa 4.

Fenomenografisen analyysin pohjalta aluksi käsitellään haastateltavien yleistä tietämystä vahvasta tunnistautumisesta sekä haastateltavien mieluisimpia maksuvälineitä. Mieluisin maksuväline oli verkkopankkimaksaminen ja MobilePay. Kuten tässäkin aineistossa, myös aiemmassa kirjallisuudessa verkkopankkimaksaminen oli suosituin maksuväline. Samaisessa tutkimuksessa mobiilimaksaminen oli vasta viidenneksi suosituin maksutapa sekä mieluisimmassa maksutavassa että sen todetussa käytössä. (Borgström, Launo, Majaniemi, Oksanen & Tikkanen, 2020). Tutkimus eroaa hieman tästä lähteestä, sillä mobiilimaksaminen on lähes yhtä suosittu kuin verkkopankkimaksaminen, vaikka

haastatteluun valittiin henkilöitä, joiden mieluisin maksutapa on nyt tai joskus ollut pankkikortilla maksaminen. Tutkimuksen aineisto vastaa enemmän Hakalan (2021) aineistoa, jossa mobiilimaksaminen on saanut 53 prosenttia ja verkkopankkimaksaminen 29 prosenttia annetuista äänistä mieluisimman maksutavan äänestyksessä. Tämän tutkimuksen otanta on hyvin pieni, vain kahdeksan haastateltavaa, joten mitään suuria johtopäätöksiä tästä ei kuitenkaan voi tehdä.

Vahva tunnistautuminen oli haastateltaville tuttu asia. He olivat törmänneet siihen maksaessaan pankkikortilla verkko-ostoja. He tiesivät, että vahva tunnistautuminen tarkoittaa oikean käyttäjän tunnistamista verkkopankkitunnuksilla, jos maksaa pankkikortilla ostoja verkossa. Vahvaa tunnistautumista on kuitenkin myös muissa maksutavoissa. Tunnistusmenetelmässä on käytettävä käyttäjän tiedossa olevan todentamistekijän, eli pankkikortin tai käyttäjätunnusten lisäksi myös joko käyttäjän hallussa olevaa laitetta, kuten puhelinta tai luontaista todentamistekijää, kuten kasvontunnistusta tai sormenjälkitunnistusta. (Finanssivalvonta, 2019b). Tämä tarkoittaa käytännössä esimerkiksi sitä, että mobiilimaksusovelluksella kuten MobilePaylla maksaessaan käyttäjän ei tarvitse erikseen tunnistautua verkkopankkitunnuksilla, koska vahva tunnistautuminen täyttyy käytettäessä puhelinta maksamiseen.

Vahvan tunnistautumisen kokemuksesta ei löytynyt aikaisempaa tutkimusta, joten tätä aihetta oli syytä tutkia. Ensimmäinen tutkimuskysymykseni ”Miten kuluttajat ovat kokeneet vahvan tunnistautumisen käyttöönoton?” tutkii kuluttajien kokemuksia vahvan tunnistautumisen käyttöönotosta. Haastattelijoiden kokemusten perusteella haastateltavat ovat kokeneet vahvan tunnistautumisen pankkikortilla maksaessa kovin helppokäyttöiseksi, mutta samaan aikaan heitä on turhauttanut se, kun vahvan tunnistautumisen tultua osaksi pankkikorttimaksua, pankkikortista on tullut täysin turha maksuväline. Siinä täytyy tehdä sama toimenpide kuin verkkopankkimaksussa, mutta sen lisäksi ensin pitää syöttää kortin tiedot. UTAUT2-mallin vaivannäön odotukset täyttyvät osittain, sillä teknologia on helppokäyttöistä, mutta käyttäjän kokiessa sen melko turhaksi, vaivannäön odotukset kärsivät. Koettu helppokäyttöisyys ja vaivannäön odotukset ovat kuitenkin käyttöaikomuksen yksiä tärkeimmistä tekijöistä, joten tämä on yksi suurimmista tekijöistä, miksi pankkikorttimaksamista on vähennetty ja näin ollen vahvaa tunnistautumista ei ole otettu käyttöön. Kuten haastatteluista kävi ilmi, maksukäyttäytyminen on menossa siihen suuntaan, että käytetään sellaisia maksuvälineitä, joissa vahva tunnistautuminen kuuluu prosessiin itsestään, eikä sellaiseen, missä pitää erikseen käydä verkkopankkitunnuksilla tunnistautumassa. Samaa mieltä on myös Alhonen (2015) sanoessaan, että maksutapojen trendi tulee olemaan mobiililaitteiden kehityksen mukaista. Vahvalla tunnistautumisella on myös haettu mobiilimaksamisen edistämistä (European Comission, 2015).

Suorituskyvyn odotukset ovat vaivannäön odotusten ohella myös tärkeitä tekijöitä UTAUT2-mallissa (Venkatesh ym., 2012). Uuden teknologian käyttöönottamisessa onkin hyvä miettiä, miksi tämä pitää tehdä tällä tavalla ja mitä hyötyä siitä on. Haastatteluissa kävi ilmi, että kuluttajat pohtivat asian syvällistä tarkoitusta silloin, kun vahva tunnistautuminen tuli. Haastatteluiden perusteella vahvassa tunnistautumisessa on selkeästi yleisellä tasolla havaittava hyöty, joka on käyttäjän turvallisuus. Haastateltavat eivät olleet kokeneet sitä henkilökohtaiseksi, mutta siitä on hyötyä esimerkiksi, jos pankkikortti katoaa ja sen löytää sellainen henkilö, joka mahdollisesti voisi käyttää pankkikorttia omiin ostoksiin, niin vahvalla tunnistautumisella on poistettu yksi mahdollinen väärinkäyttömahdollisuus, joka on verkosta tilaaminen. Myös toinen hyöty tuli ilmi haastatteluista, kun pankkikortilla maksaa, niin tunnistautumisvaiheessa järjestelmä ilmoittaa, mihin maksu on menossa. Tämä tuo myöskin kuluttajalle turvallisuuden tuntua, kun näkee, että rahat ovat menossa oikeaan osoitteeseen.

UTAUT2-malliin lisättiin uskottavuus yhdeksi teknologian käyttöönoton käyttöaikomuksen tekijäksi. Uskottavuus käsittelee uuden teknologian turvallisuus- ja yksityisyysuhkia. Vahva tunnistautuminen on säädetty edistämään käyttäjän turvallisuutta (European Comission, 2015). Haastatteluista selvisi, että kuluttajat kokevat vahvan tunnistautumisen turvallisuutta edistävänä teknologiana. Melkein kaikki luottavat tunnistautumisjärjestelmään, mutta yksi haastateltavista yrittää välttää tunnistautumista mahdollisimman paljon, mutta käyttää kuitenkin pankkitunnuksilla tunnistautumista silloin kun ei ole mahdollista kiertää sitä.

Seuraavassa UTAUT2-mallin käyttöönoton aikomuksen edeltävissä tekijöissä käydään läpi sosiaalista vaikutusta (Venkatesh ym., 2012). Se on kuluttajan läheisten mielipiteitä, jotka vaikuttavat käyttöönoton aikomukseen. Haastatteluiden perusteella kuluttajat eivät ole keskustelleet vahvasta tunnistautumisesta läheistensä kanssa, joten tämä tekijä ei auttanut vahvan tunnistautumisen käyttöönottoon millään tavalla, ei positiivisesti eikä negatiivisesti.

Helpottavat olosuhteet ovat Venkateshin ym. (2012) UTAUT2-mallissa sellaisia tekijöitä, jotka auttavat ja helpottavat käyttäjää teknologian käyttöönotossa. Tekijöitä ovat muun muassa taidot ja erilaiset laitteet. Haastatteluissa tällaisia ilmeni, että teknologiaosaaminen on koettu vaikuttaneen positiivisesti vahvan tunnistautumisen käyttöönotossa. Jotkut ihmettelivät sitä, että onkohan mahdollista sellainen tilanne, että vahvan tunnistautumisen teknologiaa ei osaisi käyttää. Yksi haastateltavista ajatteli teknologiaosaamisen vaikuttaneen siihen, että osaa käyttää myös muita helpottavia tekijöitä, kuten automaattista tunnusten täyttämistä ja biometristä tunnistautumista. Helpottavaksi teknologiaksi haastatteluissa paljastuikin juuri nämä teknologiat, joita kuluttajat käyttävät vahvaa tunnistautumista käyttäessä. Raka ym. (2019) sanovat automaattisen tietojen täyttämisen nopeuttavan maksutapahtumaa, mutta samoin se nopeuttaa myös vahvaa tunnistautumista. Heidän mukaansa se on nykyään myös turvallista.

Haastateltavat olivat tottuneet vahvaan tunnistautumiseen varsin hyvin, osin myös tottunut välttelemään vahvaa tunnistautumista. Tämä johtuu asenteesta sitä kohtaan ja siitä, että vahvaa tunnistautumista on helppo käyttää. Asennetta kuvataan jo Davisin (1985) luomassa TAM-mallissa koetun hyödyllisyyden ja koetun helppokäyttöisyyden summana. Jos käyttäjä kokee teknologian helppokäyttöiseksi ja hyödylliseksi, hänen asenteensa sitä kohtaan on hyvin todennäköisesti myös positiivinen. (Davis, 1985). Haastatteluissa asenne olikin hyvin hajanaista. Kuluttajien asenne oli positiivista, neutraalia ja negatiivista. Negatiivinen asenne johtui siitä, että haastateltava koki vahvan tunnistautumisen turhaksi, josta ei ole hyötyä ja positiivinen asenne johtui siitä, että haastateltava koki turvallisuuden olevan ehdottoman tärkeä ja siksi oli hyvä asenne sitä kohtaan. Neutraali asenne puolestaan tarkoitti sitä, että haastateltava käyttää teknologiaa, ja se ei erityisesti ärsytä häntä, mutta ymmärtää hyvin, miksi se on tullut osaksi verkkomaksamista.

UTAUT2-mallissa on kolme moderaattoria: ikä, sukupuoli ja kokemus. Tutkimuksen haastateltavien määrä oli liian pieni verratakseen tuloksia moderaattoreiden suhteen. Lisäksi laadullisessa tutkimuksessa ei ole tarkoituksena tehdä vertailua. Ikähaitari oli rajattu tarkoituksellisesti, joten sen vaihteluväli on liian pieni tulosten vertaamiseksi. Sukupuolesta voidaan sanoa vain se, että heidän kokemuksensa ja perustelunsa eivät olleet mitenkään riippuvaisia sukupuolesta. Naiset, joita oli vähemmän, eivät erotu joukosta mitenkään muuten, kuin kysyttäessä sukupuolta. Teknologinen osaaminen eli kokemus puolestaan saattaa vaikuttaa hieman siihen, miten paljon ymmärtää teknologiasta ja miten käyttää termejä. Venkatesh ym. (2003) kertoivat, että sukupuoli ja ikä eivät ole enää vaikuttavia moderaattoreita nuoressa sukupolvessa, joka on kasvanut ja kouluttautunut digitaalisen aikakauden aikana. Tutkimukseni vahvisti tätä kantaa hyvin voimakkaasti.

Tulevaisuudessa tämä ikäluokka siirtyy vanhempaan ikäluokkaan, mutta teknologiset taidot pysyvät, joten sukupuoli- ja ikämoderaattorit häviävät kokonaan, kun sellaisia ihmisiä ei enää ole, ketkä olisivat eläneet ilman digitaalista lapsuutta ja kasvatusta.

Toinen tutkimuskysymys (”Miten vahvan tunnistautumisen on koettu vaikuttavan maksukäyttäytymiseen?”) käsittelee vahvan tunnistautumisen aiheuttamaa maksukäyttäytymisen muutosta. Vahva tunnistautuminen on vaikuttanut puoliin haastateltavista siten, että ovat jättäneet pankkikorttimaksamisen kokonaan pois tai vähentänyt sitä. Suurin osa heistä on myös ottanut uutena maksutapana käyttönsä MobilePayn. Haastateltavat ovat jättäneet pankkikortin pois, koska kokevat sen täysin turhaksi ja hitaaksi maksutavaksi. Puolestaan MobilePaysta he kertovat sen olevan nopea ja helppo tapa maksaa verkko-ostokset. Nämä ovat täysin linjassa Karin (2020) tilastojen kanssa, sillä MobilePaylla tehty maksutapahtuma on keskimäärin yli kolme kertaa nopeampi kuin pankkikortilla tehty maksutapahtuma (katso kuvio 5). Myös Borgströmin ym. (2020) tutkimuksessa suomalaisten maksukäyttäytymisestä MobilePay oli ylivoimaisesti äänestetty helpoimmaksi ja nopeimmaksi maksuvälineeksi kaikista välineistä.

Tulokset osoittivat, että pankkikortilla maksaminen on omaksuttu melko huonosti pankkikortilla maksaessa. Tämä tarkoittaa liiketoiminnallisesta näkökulmasta sitä, että kauppiaiden ei kannata verkossa panostaa tulevaisuudessa pankkikorttimaksamiseen niin paljoa, vaan heidän kannattaa tarjota uusia maksutapoja, kuten MobilePayta, joka on Suomessa melko suosittu. Se on saanut viime vuosien aikana nuorten ja nuorten aikuisten keskuudessa valtavaa suosiota. Kuten Wikholm (2019) kertoo kuviossa 6, kauppiaiden on syytä panostaa maksutapojen määrään, helppouteen ja hintaan.

7.2 Tutkimuksen luotettavuus, rajoitukset ja jatkotutkimusaiheet

Tutkimuksen luotettavuus koostuu monesta tekijästä: Ensinnäkin tutkimuksen empiirinen osuus on suunniteltu huolella ja haastattelussa on käytetty koehaastateltavaa, jolloin haastattelun runkoa tarkasteltiin vielä paremmaksi, jotta saadaan haastateltavilta mahdollisimman subjektiivisia vastauksia ja tutkimuskysymyksiin vastaavia vastauksia. Toiseksi tutkimus on uskottava, sillä tutkimuksessa on kahdeksan eri henkilön kokemuksia ja siten myös yleisimmät kokemukset tulee helpommin esiin. Lisäksi tutkimuksen haastateltavat olivat osin tutkimuksen tekijälle tuttuja, mutta kaikki eivät olleet, koska käytin lumipalloefektiä haastateltavien keräämisessä. Riippuvuutta haastateltavien välillä ei täten ollut. Kysymykset on laadittu ja haastateltavat on kerätty riippumattomasti rajaus huomioiden.

Haastatteluissa ilmeni jonkin verran samanlaisia kokemuksia. Eroavaisuuksia haastateltavien välillä löytyi hyvin, joten fenomenografinen analyysi oli oikea valinta tutkielmaan. Ensimmäinen haastateltava toimi koehaastateltavana, joten hänelle esitetyt kysymykset erosivat hieman muista, mutta suuria eroja ei vastauksissa siltikään näkynyt.

Tutkielman rajoituksena on haastatteluiden pituudet. Keskimäärin 20 minuutin haastattelut ovat todella lyhyitä laadullisen haastattelun tutkimukseen, jossa kerätään haastateltavilta kokemuksia aiheesta. Kysymykset olivat tarkkaan aseteltuja ja niitä oli melko laajasti, mutta vastausten lyhyys silti yllätti. Toisena rajoittavana tekijänä oli löytyneen kirjallisuuden vähyys vahvan tunnistautumisen omaksumisesta, joten tutkimuksen tuloksien peilaaminen aiempaan tutkimukseen oli vajavaista.

Ensimmäisenä jatkotutkimusaiheena esitetään haastatteluissa ilmennyt ongelma, joka johtuu vahvan tunnistautumisen tuomasta turvallisuuden tunteesta. Osa

haastateltavista koki turvallisuuden tunnetta vahvasta tunnistautumisesta, ja he eivät koe enää riskiä menettää rahojaan, jos heidän pankkikorttinsa esimerkiksi katoaa. Vaikka vahva tunnistautuminen poistaa yhden mahdollisen väärinkäytön, jäljelle jää lukematto-mia muita vaihtoehtoja.

Toisena jatkotutkimusaiheena esitetään maksukäyttäytymisen muutoksesta tehtä-vää määrällistä tutkimusta, joka tutkii eri ikäryhmien välisiä eroja maksutavan valinnassa ja miten se on muuttunut viimeisen viiden vuoden aikana ja ennustuksia siitä, miten se tulee muuttumaan jatkossa. Maksutapojen käytöstä ei löytynyt vuoden 2021 osalta juuri-kaan tilastoja tai tutkittua tietoa, joten siinä oli iso aukko, ottaen huomioon, että vahva tunnistautuminen on tullut pankkikorttimaksuihin juuri kyseisenä vuonna.

Kolmas jatkotutkimusaihe on käyttäjien kokemusten tutkiminen sähköisen kuitti-palvelun yhdistämisestä mobiililompakkoon. Onko tämä tekijä, jonka takia kuluttajat käyttävät mobiililompakkoa, tai voisivat käyttää mobiililompakkoa?

Neljäs ja viimeinen jatkotutkimusaiheeni koskee vahvan tunnistautumisen omaksu-mista eri ikäluokissa. Ikä- ja sukupuolimoderaattoreiden vaikutus voi korostua tutkimalla eri ikäluokissa vielä jonkin aikaa, kun täällä on vielä montaa eri sukupolvea, jotka eivät ole yhdenvertaisessa asemassa teknologian käyttöönoton kanssa. Tämä aikakausi kestää vielä monta kymmentä vuotta, joten tutkimukselle on hyötyä pitkäksi aikaa ja siitä saa varmasti monet hyötyä omiin projekteihinsa.

8 YHTEENVETO

Tämä tutkimus oli jaettu kahteen eri osaan, jotka olivat kirjallisuuskatsaus ja empiirinen osio. Kirjallisuuskatsauksessa pureuduin vahvan tunnistautumisen omaksumiseen verkko-ostoissa. EU:n säätämä toinen maksupalveludirektiivi PSD2 tuli voimaan 2019 syyskuussa, sisältäen pankkikorttimaksuun pakolliseksi lisättävän vahvan tunnistautumisen. Tämä muutos sai kuitenkin lisäaikaa vuoden 2020 loppuun saakka ja nyt olemme eläneet reilun vuoden vahvan tunnistautumisen aikaa. Tutkimuksen aihe perustuu kyseisen vahvan tunnistautumisen omaksumiseen nyt, kun se on ollut kuluttajilla yli vuoden käytössään.

Tutkielman toisessa luvussa käsiteltiin teoriaa, johon tutkimus perustuu. Teknologian hyväksyminen toimi tämän tutkimuksen teoriaviitekehyksenä. Tutkimus pohjautui TAM-malliin sekä UTAUT2-malliin. TAM-malli esittää teknologian käyttöönotossa olevan kaksi eri määräävää tekijää. Ne ovat koettu helppokäyttöisyys ja koettu hyödyllisyys. UTAUT2-mallin mukaan teknologian käyttöönotossa on monia eri tekijöitä, jotka vaikuttavat siihen, otetaanko teknologiaa käyttöön, eli omaksuuko käyttäjä sen. Näitä tekijöitä ovat suorituskyvyn odotukset, vaivannäön odotukset, sosiaalinen vaikutus, helpottavat olosuhteet, hinta-arvo, koettu nautinto ja tottumus. Mallia muokattiin tähän tutkimukseen sopivaksi poistamalla hinta-arvon, koska vahvan tunnistautumisen käyttö ei maksa käyttäjälle mitään ja lisäämällä uskottavuuden, joka käsittelee käyttäjän kokemaa turvallisuutta teknologiassa.

Kolmannessa luvussa käsiteltiin maksuvälineitä. Suomessa yleisiä maksuvälineitä ovat verkkopankkimaksu, pankkikorttimaksu, laskulla maksaminen, mobiilimaksaminen ja PayPal. Verkkopankkimaksaminen on selvästi suosituin maksuväline ja mobiilimaksaminen on nostanut suosiotaan viime vuosien aikana.

Neljännessä luvussa käsiteltiin toista maksupalveludirektiiviä (PSD2). Uusina asioina toisessa maksupalveludirektiivissä ovat maksutapahtumassa kolmansien osapuolten tuominen sääntelyn piiriin sekä pakolliseksi verkkomaksuihin tullut vahva tunnistautuminen. Tämä tutkielma keskittyi vahvaan tunnistautumiseen, mutta luvussa esiteltiin lyhyesti myös muut maksupalveludirektiivin uudistukset.

Tämän tutkielman empiirisessä osiossa tarkoituksena oli tutkia kuluttajien kokemuksia vahvan tunnistautumisen omaksumisesta ja siitä, miten vahva tunnistautuminen on koettu vaikuttaneen heidän maksukäyttäytymiseensä. Vahvan tunnistautumisen omaksumisesta tai kuluttajien kokemuksista ei löytynyt tutkittua tietoa, joten tutkimuksella on tarkoitus tuottaa tutkimusta tästä aiheesta.

Empiirisen tutkimuksen haastattelurunko ja kysymykset pohjautuivat UTAUT2-teoriaan. Haastattelu toteutettiin puolistrukturoidulla menetelmällä, missä haastateltiin kahdeksaa nuorta aikuista, jotka olivat tehneet verkko-ostoja riittävästi osallistuakseen haastatteluun. Haastattelut tallennettiin ja litteroitiin, jonka jälkeen ne vielä teemoiteltiin. Tulokset analysoitiin fenomenografisen analyysin avulla.

Ensimmäinen tutkimuskysymys oli:

- Miten kuluttajat ovat kokeneet vahvan tunnistautumisen käyttöönoton?

Haastateltavien kokemuksen perusteella he tiesivät, mikä vahva tunnistautuminen on ja he yhdistivät sen verkkokaupassa pankkikortilla maksamisen yhteydessä vaadittavaan pankkitunnuksilla tunnistautumiseen. He kokivat vahvan tunnistautumisen olevan helppokäyttöinen, mutta turha välivaihe, joka tekee myös pankkikortilla verkossa maksamisesta turhan. Kuluttajien asenne vahvaa tunnistautumista kohtaan vaihteli. Suurimmalla osalla oli joko, positiivinen tai neutraali asenne sitä kohtaan, mutta osalla oli myös hyvinkin kielteinen asenne vahvaa tunnistautumista kohtaan. Positiivinen asenne tarkoittaa yleensä sitä, että kuluttaja kokee turvallisuuden olevan tärkeää hänelle verkosta ostaessa. Neutraali asenne puolestaan yhdistyy sellaisiin kuluttajiin, joita vahva tunnistautuminen ei ärsytä, mutta eivät myöskään koe siitä olevan paljoa hyötyä. Lisäksi he ymmärtävät miksi se on tullut osaksi maksujärjestelmää. Kielteinen asenne tarkoittaa sitä, että kuluttaja ei näe vahvassa tunnistautumisessa kovin paljoa järkeä, vaan ajattelee sen olevan enemmän yhden maksutavan tuhoamista.

Toinen tutkimuskysymys oli:

- Miten vahva tunnistautuminen on koettu vaikuttavan maksukäyttäytymiseen?

Tähän kysymykseen haastateltavilta saatiin melko selkeä vastaus: kuluttajat ovat vähentäneet pankkikortilla maksamista ja lisänneet MobilePay-maksamista vahvan tunnistautumisen takia. Syynä pankkikorttimaksamisen vähentämiseen oli hitaus ja ylimääräinen vaihe. MobilePayn lisäämisen syynä oli puolestaan nopeus ja helppous.

LÄHTEET

Abbott, J., & Patil, S. (2020, April). How mandatory second factor affects the authentication user experience. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-13).

Alhonen A. (2015). Verkkokauppaopas, 68-79.

Aydin, G., & Burnaz, S. (2016). Adoption of mobile payment systems: A study on mobile wallets. Journal of Business Economics and Finance, 5(1), 73-92.

Bartłomiejczyk, M., El Fray, I., Kurkowski, M., Szymoniak, S., & Siedlecka-Lamch, O. (2022). User Authentication Protocol Based on the Location Factor for a Mobile Environment. IEEE Access, 10, 16439-16455.

Bezovski, Z. (2016). The future of the mobile payment as electronic payment system. European Journal of Business and Management, 8(8), 127-132.

Borgström, S., Launo, M., Majaniemi, P., Oksanen, M. & Tikkanen, S. (2020). Verkkokauppa Suomessa 2020. Haettu 2.3.2022 osoitteesta https://www.paytrail.com/raportti/verkkokauppa-suomessa-2020

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management science, 35(8), 982-1003.

Erdogmus, N., & Marcel, S. (2014). Spoofing face recognition with 3D masks. IEEE transactions on information forensics and security, 9(7), 1084-1097.

Euroopan unioni (2015). Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366. Annettu 25.11.2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY,2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta. Haettu 3.3.2022 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32015L2366&from=EN#d1e5625-35-1

Euroopan unioni (2021). Asetukset, direktiivit ja muut säädökset. Haettu 28.2.2022 osoitteesta https://european-union.europa.eu/institutions-law-budget/law/types-legislation_fi

European Comission (2015). European Parliament adopts European Commission proposal to create safer and more innovative European payments. Haettu 28.2.2022 osoitteesta https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5792

Fabcic, D. (2020). Strong Customer Authentication in Online Payments Under GDPR and PSD2: A Case of Cumulative Application. In IFIP International Summer School on Privacy and Identity Management (pp. 78-95). Springer, Cham.

Finanssivalvonta (2019a). Finanssivalvonta sallii tilapäisiä helpotuksia vahvan tunnistamisen toteuttamiseen verkkokaupan toteuttamiseen verkkokaupan korttimaksamisessa. Haettu 23.3.2022 osoitteesta https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2019/finanssivalvonta-sallii-tilapaisia-helpotuksia-vahvan-tunnistamisen-toteuttamiseen-verkkokaupan-korttimaksamisessa/

Finanssivalvonta (2019b). Finanssivalvonta noudattaa EBAn esittämää vahvan tunnistamisen lisäaikaa verkkokaupan korttimaksamisessa – vaatimukset toteutettava 31.12.2020 mennessä. Haettu 22.3.2022 osoitteesta https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2019/finanssivalvonta-noudattaa-eban-esittamaa-vahvan-tunnistamisen-lisaaikaa-verkkokaupan-korttimaksamisessa--vaatimukset-toteutettava-31.12.2020-mennessa/

Finanssivalvonta (2019c). PSD2. Päivitetty 25.3.2019. Haettu 3.3.2022 osoitteesta https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/psd2/

Finlex (2009). 7.8.2009/617, Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. Haettu 8.3.2022 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2009/20090617

Finlex (2017). 898/2017, Laki maksupalvelulain muuttamisesta. Laadittu 14.12.2017. Haettu 3.3.2022 osoitteesta https://www.finlex.fi/fi/laki/alkup/2017/20170898#Pidm45237816123904

Fishbein, M., & Ajzen, I. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prenti ce-Hall.

Fishbein, M., Ajzen, I., & Belief, A. (1975). Intention and Behavior: An introduction to theory and research.

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. Australian & New Zealand Journal of Psychiatry, 36(6), 717-732.

Galbally, J., & Satta, R. (2016). Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. IET Biometrics, 5(2), 83-91.

Gupta, E., Agarwal, M., & Sivakumar, R. (2020, June). Blink to get in: Biometric authentication for mobile devices using eeg signals. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

Hakala, H. (2021). Miten suomalaiset maksavat verkossa 2021? Julkaistu 18.2.2021. Haettu 2.3.2022 osoitteesta https://www.paytrail.com/blog/miten-suomalaiset-maksavat-verkossa-2021

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., & Hasan, A. M. (2020, February). A review of user authentication model for online banking system based on mobile IMEI number. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012061). IOP Publishing.

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). Mobile payments: Consumer benefits & new privacy concerns. Available at SSRN 2045580.

Hsu, H. H., & Chang, Y. Y. (2013). Extended TAM model: Impacts of convenience on acceptance and use of Moodle. Online Submission, 3(4), 211-218.

Huttunen, K. (2019). Verkkokaupan maksutavat. Haettu 3.2.2022 osoitteesta https://www.zoner.fi/verkkokaupan-perustaminen/maksutavat/

Hyppönen, M. (2021). Internet. Biometriikka.

Kang, J. (2018). Mobile payment in Fintech environment: trends, security challenges, and services. Human-centric Computing and Information sciences, 8(1), 1-16.

Kari, J. (2020). MobilePay ylivoimaisesti nopein maksutapa – katso vertailu. Julkaistu 21.12.2020. Haettu 2.3.2022 osoitteesta https://www.paytrail.com/blog/mobilepay-ylivoimaisesti-nopein-maksutapa-katso-vertailu

Kunda, D., & Chishimba, M. (2018). A survey of android mobile phone authentication schemes. Mobile Networks and Applications, 1-9.

Kyberturvallisuuskeskus (2021). Vahva (pankki)tunnistus asiointipalveluissa muuttuu viimeistään 1.10.2019. Haettu 21.3.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/vahva-pankkitunnistus-asiointipalveluissa-muuttuu-viimeistaan

Mobiilivarmenne (2022). Näin käytät Mobiilivarmennetta. Haettu 21.3.2022 osoitteesta https://mobiilivarmenne.fi/nain-se-toimii/

Możdżyński, D. (2017). The conceptions of new payment methods based on revised payment services directive (PSD2). *Information Systems in Management*, *6*.

Naik, N., & Jenkins, P. (2017, May). Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect. In 2017 11th International Conference on Research Challenges in Information Science (RCIS) (pp. 163-174). IEEE.

Niranjanamurthy, M. (2014). E-commerce: Recommended online payment method-Paypal. International journal of computer science and mobile computing, 3(7), 669-679.

Palau-Saumell, R., Forgas-Coll, S., Sánchez-García, J., & Robres, E. (2019). User acceptance of mobile apps for restaurants: An expanded and extended UTAUT-2. Sustainability, 11(4), 1210.

Park, H. S. (2000). Relationships among attitudes and subjective norms: Testing the theory of reasoned action across cultures. Communication Studies, 51(2), 162-175.

Pyyalampi, S. (2021). Verkkokaupan maksunvälityspalvelut vertailussa. Haettu 13.5.2022 osoitteesta https://www.kupli.fi/verkkokaupan-maksunvalityspalvelut-vertailussa/

Raka, P., Agrwal, S., Kolhe, K., Karad, A., Pujeri, R. V., Thengade, A., & Pujeri, U. (2019). OCR to read credit/debit card details to autofill forms on payment portals. Int. J. Res. Eng. Sci. Manag, 2(4), 478-481.

Rigatelli, S., Pajunen, I. & Orjala, A. (2015). Teleoperaattori sim-korttien hakkeroinnista: Yksityisasiakkailla ei syytä huoleen. Haettu 8.4.2022 osoitteesta https://yle.fi/uutiset/3-7818200

Rondan-Cataluña, F. J., Arenas-Gaitán, J., & Ramírez-Correa, P. E. (2015). A comparison of the different versions of popular technology acceptance models: A non-linear perspective. *Kybernetes*.

Scahill, J. & Begley, J. (2015). How spies stole the keys to the encryption castle. Haettu 8.4.2022 osoitteesta https://theintercept.com/2015/02/19/great-sim-heist/

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. <https://www.fsd.tuni.fi/menetelmaopetus/>. (Viitattu 10.05.2022.)

Sintonen, M., Takala, K., Hellqvist, M., & Liikanen, J. (2021). COVID-19 pandemic causing permanent change in payment habits.

S-pankki (18.2.2022). Milloin kannattaa maksaa luottokortilla? Haettu 21.4.2022 osoitteesta https://www.s-pankki.fi/fi/artikkelit/milloin-kannattaa-maksaa-luottokortilla/

Suomen virallinen tilasto (SVT) (2021a). Väestön tieto- ja viestintätekniikan käyttö. ISSN=2341-8699. 1. Verkkokauppa murroksessa. Helsinki: Tilastokeskus. Haettu 23.2.2022 verkosta osoitteesta http://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_kat_001_fi.html

Suomen virallinen tilasto (SVT) (2021b). Väestön tieto- ja viestintätekniikan käyttö. ISSN=2341-8699. 2021. Helsinki: Tilastokeskus. Haettu 5.4.2022 osoitteesta http://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_tie_001_fi.html

Suomi.fi (2022). Eri tunnistusvälineillä tunnistautuminen. Haettu 21.3.2022 osoitteesta https://www.suomi.fi/ohjeet-ja-tuki/tietoa-tunnistuksesta/eri-tunnistusvalineilla-tunnistautuminen

Van Raaij, E. M., & Schepers, J. J. (2008). The acceptance and use of a virtual learning environment in China. Computers & education, 50(3), 838-852.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. Information systems research, 11(4), 342-365.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. Decision sciences, 39(2), 273-315.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. Decision sciences, 27(3), 451-481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly, 157-178.

Wolters, P. T., & Jacobs, B. P. (2019). The security of access to accounts under the PSD2. Computer law & security review, 35(1), 29-41.

Wood, S. (2013). Generation Z as consumers: trends and innovation. Institute for Emerging Issues: NC State University, 119(9), 7767-7779.

Zhong, Y., Oh, S., & Moon, H. C. (2021). Service transformation under industry 4.0: Investigating acceptance of facial recognition payment through an extended technology acceptance model. Technology in Society, 64, 101515.

LIITE 1 HAASTATTELURUNKO

1. TAUSTATIEDOT JA TEKNOLOGINEN KOKEMUS

- Ikä?
- Sukupuoli?
- Kuinka monesti olet tehnyt ostoja verkossa:
    - Viimeisen viikon aikana?
    - Viimeisen kuukauden aikana?
- Kerro teknologiaosaamisestasi?
- Jos tulee uusi teknologinen laite, miten kiinnostunut olet sitä kohtaan?
- Jäävätkö ne käyttöösi pidemmäksi aikaa vai ovatko ne hetkellisiä testailuja?

2. MAKSUVÄLINEET

- Kuva verkkokaupan maksuvälineistä (liite 2):
- Tässä on kuva maksuvälineistä, mitä verkkokaupat yleensä tarjoavat vaihtoehdoiksi Suomessa. Mikä on mieluisin maksutapasi? ja minkä valitsisit maksutavaksi?
- Miksi valitset juuri kyseisen vaihtoehdon?
    - (Onko syynä nopeus, helppous, turvallisuus, tottumus vai joku muu?)
- Oletko maksanut pankkikortilla verkko-ostoja vuoden sisällä? Entä sitä aikaisemmin?
    - Miten olet sen kokenut?
- Miten koet maksukäyttäytymisen muuttuneen viime vuosien aikana?
    - Jos on muutoksia: Onko syynä ollut vahva tunnistautuminen?
- Koetko, että verkkokaupoilla on yleisesti tarpeeksi vaihtoehtoja tarjolla?

VAHVA TUNNISTAUTUMINEN 3-9

- Oletko kuullut vahvasta tunnistautumisesta ja oletko huomannut, että se vaaditaan nykyään verkkomaksuissa, kun maksat pankkikortilla?
    - Täydentävä vastaus:
    - Verkossa tapahtuviin pankkikorttimaksuihin tuli EU tasolta direktiivi voimaan viime vuoden alussa, minkä mukaan pankkikorttimaksuissa tarvitaan kortin tietojen lisäksi erikseen vielä vahva tunnistautuminen pankkitunnuksilla.
    - Tämä vahva tunnistautuminen tarvitaan myös muissakin maksuvaihtoehdoissa, mutta niissä, esimerkiksi mobiilimaksamisessa ja verkkopankkimaksuissa vahva tunnistautuminen tulee itsestään, kun maksamisessa käytetään matkapuhelinta tai tunnuslukulaitetta apuna.

- Tarkennan vielä, että seuraavat kysymykset koskevat verkko-ostojen yhteydessä tapahtuvaa vahvaa tunnistautumista. Eli ei esimerkiksi verottajan tai kelan sivuille kirjauduttaessa vaadittavaa tunnistautumista.

3. KOETTU HELPPOKÄYTTÖISYYS / VAIVANNÄÖN ODOTUKSET (SISÄLTÄÄ KOETUN NAUTINNON)

- Miten olet kokenut vahvan tunnistautumisen käytön pankkikortilla maksaessa?
    - Onko se ollut helppokäyttöinen?
    - Onko sen käyttö ollut mieluisaa? Tai onko niiden käyttö turhauttanut?
- Entä miten olet kokenut vahvan tunnistautumisen nykyisin käyttämässäsi maksutavassa?

4. TOTTUMUS

- Miten olet tottunut vahvan tunnistautumisen käyttöön?
- Oletko tehnyt jotain muutoksia maksukäyttäytymisessäsi vahvan tunnistautumisen takia?

5. KOETTU HYÖDYLLISYYS / SUORITUSKYVYN ODOTUKSET

- Oletko kokenut vahvasta tunnistautumisesta olevan hyötyä?

6. ASENNE

- Millainen asenne sinulla on vahvan tunnistautumisen käyttöä kohtaan?
- Millaisia tunteita se on herättänyt sinussa verkko-ostojen yhteydessä?

7. SOSIAALINEN VAIKUTUS

- Miten läheistesi mielipiteet vaikuttavat sinun suhtautumiseesi vahvaan tunnistautumiseen?
- Onko niillä ollut vaikutusta maksutavan valintaan?
- Oletko testannut jotain maksutapaa jonkun läheisesi suosituksesta?

8. HELPOTTAVAT OLOSUHTEET

- Miten koet teknologiaosaamisen vaikuttaneen vahvan tunnistautumisen käyttöön?
- Onko sinulla vahvaa tunnistautumista helpottavaa teknologiaa?
    - Esimerkiksi sormenjälkitunnistus tai kasvontunnistus

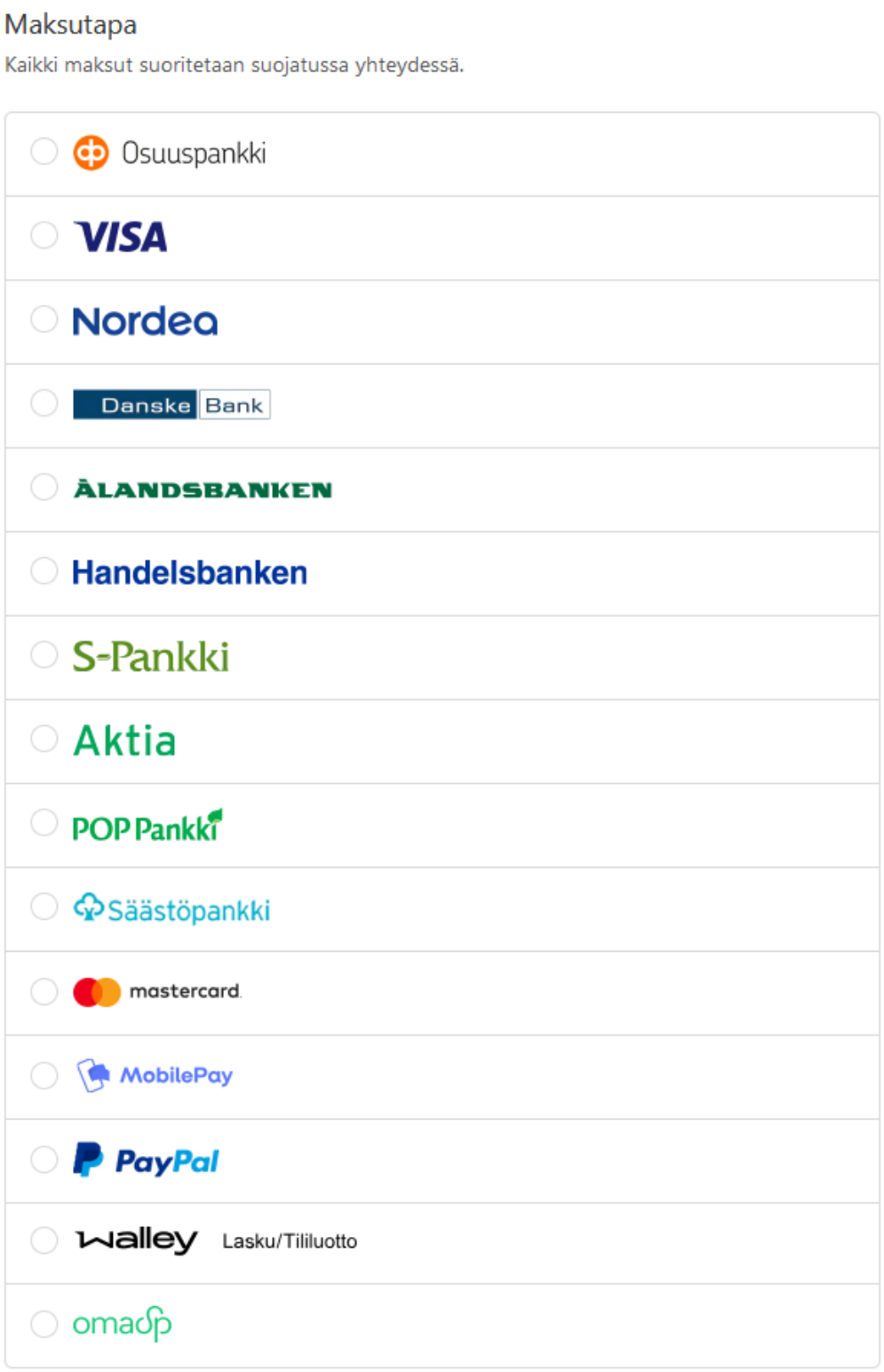
9. USKOTTAVUUS

- Koetko jotain turvallisuus- tai yksityisyysuhkia vahvassa tunnistautumisessa?
- Koetko vahvan tunnistautumisen olevat turvallisuutta edistävää teknologiaa?

10. YHTEENVETO

- Haluatko lisätä jotain?

LIITE 2 HAASTATTELUN KUVA 1



LIITE 3 HAASTATTELUISTA POISTETTU KUVA